International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Brute Force Attack on Real World Passwords

Kanakam Swathi

Student, Rajam, Vizianagaram, 532127, India.

ABSTRACT

Brute Force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks. An information system is only as secure as its weakest point. In many information systems that remains to be the human factor, in spite of continuous attempts to educate the users about the importance of password security and implementing password creation policies on them. Moreover, the users not only do the password creation and management habits remain more or less the same, but the password cracking tools, and more importantly, the computer hardware, keep improving as well. There are many types in this Brute Force Attacks. They are Simple brute force attack, Reverse brute force attack, Dictionary attack, Password Spraying brute-force attack .Password Spraying brute-force attack is considered as one of the oldest attacks in the entire history of cyber security. Amid the diverse cyber-attacks, the brute-force technique or exhaustive search has always gained its importance, when it comes to access the data in an unapproved manner. Slowly and moderately, a lot more variants of brute-force have been released by the cybercriminals as they have also evolved. Otherwise, hashing has also developed timely as a countermeasure of various cyber-attacks. The main intention of this paper is to study the different types of Brute Force Attacks.

Keywords: password cracking, Password security, force attack, dictionary attack,hashed passwords

1. Introduction

In this modern world everything is being done via internet and we keep every data which belong to us in the internet from our normal data to most confidential data. we are using internet very widely and there are also many disadvantages of it like for every coin there are both sides for using internet also there are both advantages and disadvantages cyberattack is one of thedisadvantages of it. generally, a cyber-attack is a kind of attack that targets a computer or a laptop a cyber-attack is a attempt to steal or modify original data of an individual or a data of an organization. the attacker may be an individual person or a group of people they gain unauthorized access to the computer/laptop and steal or modify the data in a cyber-attack the attacker may send a bug or a malicious software to your computer and get accesses to your computer the main motive of cyber-attack is to get the information in some attacks they will modify the information so this will cause huge potential loss to the victim and leads to cybercrimes such as theft of information and Identity. there are different types of cyber-attacks in some attacks the victim will know immediately after the attack they are called as active attacks and in some attacks the victim may not know about the attack these types of attacks are called passive attacks.

2. Literature Survey

In this paper [1] the author discussed mainly about the brute-force black-box method to attack machine learning-based systems in cyber security. We proposed a new method known as the brute-force attack method to generate AEs against machine learning based systems in cyber security. Our method is simple to implement and avoids the slow training of GAN-based attack methods. Our method generates AEs based on the confidence values of the target classifiers heuristically. Our method is a black-box attack method for which the architectures and dimensions of the target classifiers are unnecessary for attacks. The confidence values of the target models are the only required knowledge to produce AEs. The most widely used machine learning classifiers for different scenarios of cyber security are chosen as our target classifiers.

In the paper [2] From the Earlier security protocols, now we changed to IOT due to huge no of objects that max interact together in a complex manner. Hereend nodes are attached to I0T networks and communicate with a data server through a gateway. Probes that aim to obtain detailed information and brute force attacks aregeared towards guessing passwords and gaining prosperousaccess. Thedifference of this paper is the use of a time-sensitive statistical relationship approach and visualizing the attack patterns that identify its configurations in brute force attack (BFA) on an FTP service investigation.

In this paper [3] the author discussed about the mechanism of man in the middle attack and the motives behind this attack and different ways of these attacks and objectives of the attack and prevention of the attack. How the interception of the attack takes place and decryption means how the attacker initiates into the network from the sender and decrypts the connection to the receiver. How the MIMT attack is the threat to the phone communication. The most common MITM is Spoofing, there will be different types of spoofing like IP spoofing, ARP spoofing, DNS spoofing. Damage Level: The amount of damage of these attacks depends on the type of information that is being transmitted. Mostly Used WIFI connections are GSM architecture.

In this paper [4], author discussed about the sql injection attack how it can be done by the attacker and types of the attacks like inferential attack, out of band attack and blind sql injection. How these attacks effect the confidentiality, Integrity, availability of the user and effect the victim. As the sql injection attack is not known in the all cases, the author discussed about detection techniques like s Burp Suite`s vulnerability scanner, Sqlmap, Sqlninja etc. Countermeasures for sql injection attacks like Whitelisting/Blacklisting, Prepared Statement/Parameterized Query Stored Procedure etc so we can prevent the sql injection attack. Mostly used: spoof id,Tamper with existing data.

In this paper [5] the author discussed about how the cyber-attacks can be understandable easily so we can defend them easily and prevent those attacks. A password is a set of characters used for user authentication to prove identity or access approval to gainaccess to a resource which is to be kept secret from those not allowed access. Wecannot store password in plain text because of cyber threads. To secure our password from various cyber threads we use many methods and concepts like algorithms. Hashing is one of the type of algorithm which takes any size of data and turns it into a fixed-length of data. Modern Hashing Algorithm.Advantage: we can know about what are the type of attacks are going to happen and who are going to be attacked and protect them.

3. Data Collection

The dataset for the brute force attack is drawn from the Kaggle competition and represents applicants of various components. The data set contains some of the attributes.

4. Brute Force

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

A brute-force attack is a cryptanalytic attack that can, in theory, be used to attempt to decrypt any encrypted data (except for data encrypted in an information-theoretically secure manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier.

When password-guessing, this method is very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary attack are used because a brute-force search takes too long. Longer passwords, passphrases and keys have more possible values, making them exponentially more difficult to crack than shorter ones.

Brute-force attacks can be made less effective by obfuscating the data to be encoded making it more difficult for an attacker to recognize when the code has been cracked or by making the attacker do more work to test each guess. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute-force attack against it.

Brute-force attacks are an application of brute-force search, the general problem-solving technique of enumerating all candidates and checking each one. The word 'hammering' is sometimes used to describe a brute-force attack, with 'anti-hammering' for countermeasures.

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.

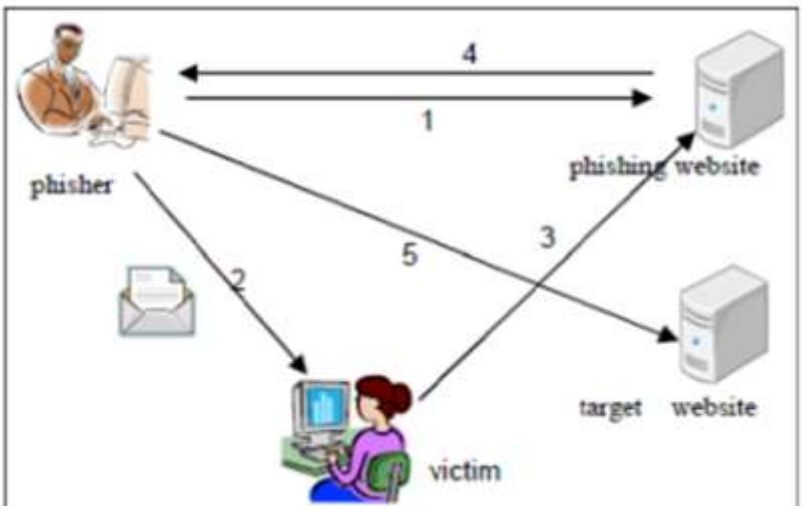
A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.

The name "brute force" comes from attackers using excessively forceful attempts to gain access to user accounts. Despite being an old cyberattack method, brute force attacks are tried and tested and remain a popular tactic with hackers.

5. Methodology

Method 1:

In paper [1], A phishing attack is a cyber-attack where the attacker will send the email and try to extract the credentials from the victim and the attacker will use the data to extract the information. The email sent to the victim will ask the login credentials for a particular website by pretending like the original website the user will give the credentials in the website thinking as original one but these credentials will be sent to the attacker and the attacker will use legitimate website to login and this will cause huge potential damage. There are different types of phishing attacks like spear phishing, whaling, pharming these are implemented on the basis of the type of person the attacker is attacking and the knowledge of the attacker also.



Spear Phishing: This variety of phishing is nearly identical to deceptive phishing. The only difference is the target. Unlike deceptive Spear Phishing spear phishing targets one individual only. The attackeraims at one person and attracts him/her into providing confidential data. The scammers customize the email according to the individual.

Whaling: Whaling attacks will occur when the phisher targets an individual at an executive position like CEO. The attacker would be profiling the victim for a particular period before performing the attack. The attacker, similar to other types, would send an email to the target person and manipulate him/her into providing information to the attacker.There are also anti phishing techniques to stop and be aware of the phishing like tools and detectors to prevent from phishing like The Computer Vision (CV) tool called Speed up Robust Features (SURF) detector and also vector machines like svm vector detector to detect the mail is malicious or not if malicious it will give us an alert to stop the mail links from navigating.

Method 2:

In paper [2], Man-in-the-middle-attack also known/abbreviated as MIM, MitM or MITMA is a type of cryptographic attack over a communication channel by a malicious third party where he/she takes over a confidential/personal communication channel between two or more communicative points or parties. In this cyber-attack, the attacker can control (read, modify, intercept, change or replace) the communication traffic between the two victims. But by using MITM protocol the unauthenticated attacker leaves any clues of his interception of this cybercrime.; the attacker remains invisible to the victims.

A man-in-the-middle attack is a type of searching attack, where attackers interrupt an existing conversation or data transfer. After inserting themselves in the middle of the transfer, the attackers pretend to be both appropriateparticipants. In this attack mainly confidentiality of the both sender and receiver will lose their confidentiality because the attacker will be able to monitor whole data of them. A man-in-the-middle attack allows a malicious character to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. One case of man-in-the-middle attacks is dynamic eavesdropping, in which the attacker makes independent associations with the victims and transfers messages between them to control them and to trust they are talking straightforwardly to each other over a private association when in certainty the whole discussion is controlled by the attacker.

Method 3:

In paper [3], A SQLi attack happens when an attacker exploits a susceptibility in the web app's SQL implementation by submitting a malicious SQL statement via a fillable field. In other words, the attacker will add code to a field to alter data or access the backend. A strong malicious SQL statement could give an administrator access to a database for the attacker by allowing them to select data such as employee ID and password combinations. They can delete, modify or dump data into the database they choose. The right SQL injection attack can allow access to a host operating system and other network resources, depending on the nature of the SQL database.SQL injection is a common attack vector that allows users with malicious SQL code to access private information by changing the backend of databases. This data may include susceptible business information, private customer details, or user details. A successful SQL injection can result in deletion of entire databases, unauthorized use of sensitive data, and unexpected granting of administrative rights to a database. This type of SQL injection attacks varies depending on the kind of database systems. The SQLi attack works on dynamic SQL statements, which are created at run time using a URI query string or web form. For example, a simple web application with a login form will allow a user email address and password. It will then allow to submit that data to a PHP file. There is a "remember me" checkbox in most forms indicating that the data from the login session will be stored in a cookie. Depending on how the statements are written in the backend for checking user ID, it may or may not be sanitized. This example statement is vulnerable and is not sanitized.

SELECT * FROM users WHERE email = $_POST['email'] AND password = md5($_POST['password']); This is because although the password is encrypted, the code directly uses the values of the $_POST [] array.

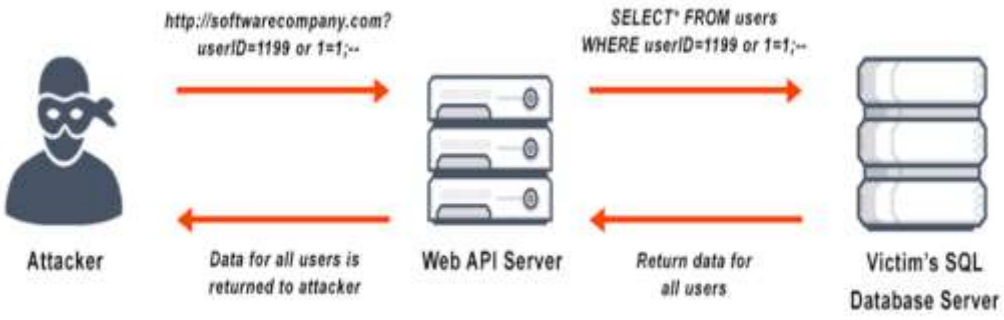
If the administrator should use "admin@company.com" and "password", like this:

SELECT * FROM users WHERE email = 'admin@company.com' AND password = md5('password');

An SQLi attacker simply needs to comment out the password portion and add a condition that will always be true, such as "1 = 1".

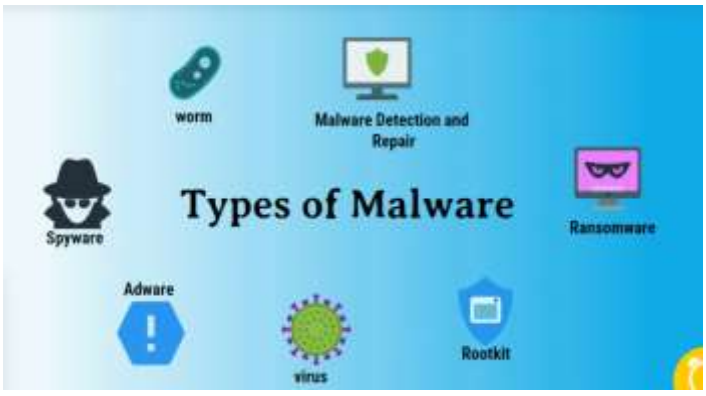
This creates a dynamic statement that ends with a condition that will always be true, defeating the security measures in place:

SELECT * FROM users WHERE email = 'xxx@xxx.xxx' OR 1 = 1 LIMIT 1 -- '] AND password = md5('password



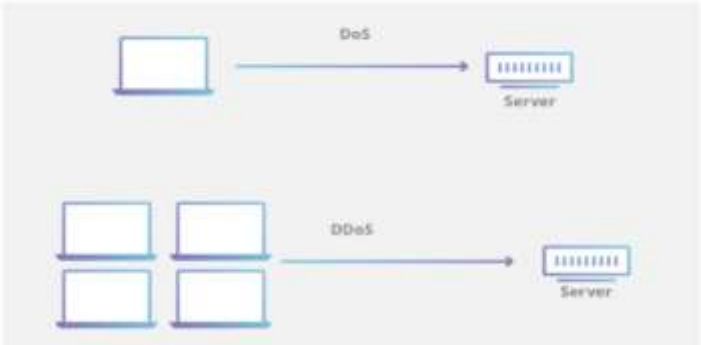
Method 4:

- Malware attack is a class of cyberattack in which malicious software is installed into the user's computer without any consent of the user. This is what we called now as virus, spyware or ransomware etc. Malicious code is attached to the legitimate code, get propagated and executed by themselves. Malwares are able to access private network, interrupt certain computing operation, steal sensitive information or any other user data and thereby making money illicitly from the target. Now a day, malware aims more at business or financial information than any credential personal information.
- In comparing to other cyber-attacks malware is very dangerous because it can attack be in different forms so we cannot detect them easily



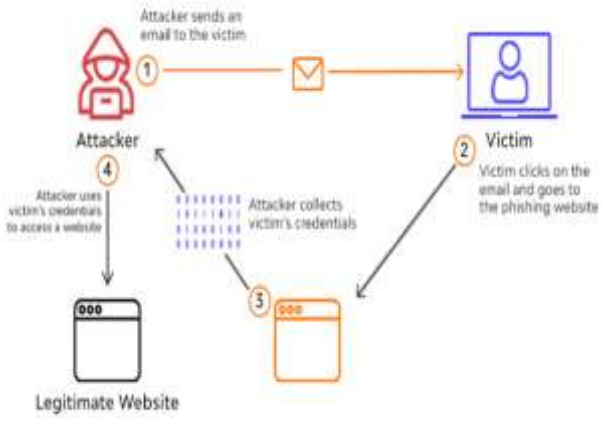
Method 5:

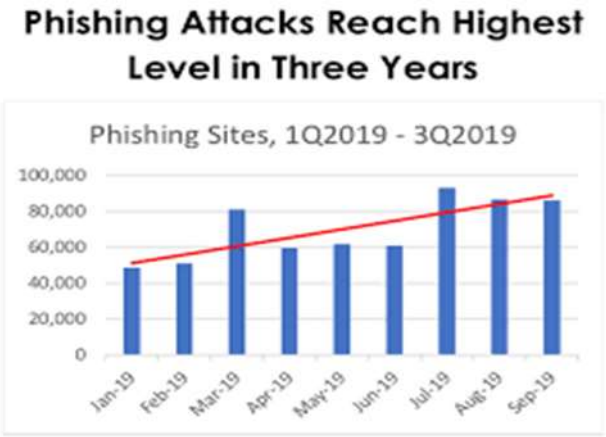
- A denial-of-service (DoS) attack is a type of cyber-attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.
- A DDoS attack is launched from numerous compromised devices, often distributed globally in what is referred to as a botnet. It is distinct from other denial of service (DoS) attacks, in that it uses a single Internet-connected device (one network connection) to flood a target with malicious traffic. There are different type of attacks in the DDos are volume-based attacks, protocol attacks etc
- The main motive behind the ddos attacks can be ideology, boredom, extortion, cyber warfare, Business feuds etc.



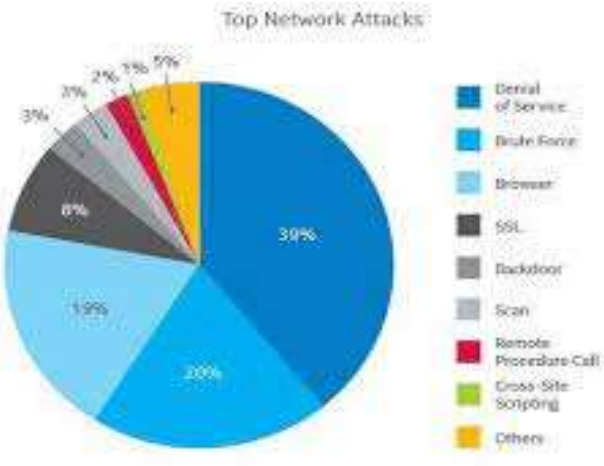
6. Results and Discussion

6.1 Phishing is a technique to gather sensitive information about the target using malicious links and emails. It is one of the most dangerous cyber-attacks that occurs in organizations, personal devices, etc. It is often difficult to distinguish between genuine emails and phishing emails. There are several methods that can be used to avoid this attack. Periodical updating of anti-phishing tools and platforms can prove to be very powerful. there are some prevention techniques to prevent them also so we should use those prevention tools and try to avoid them.





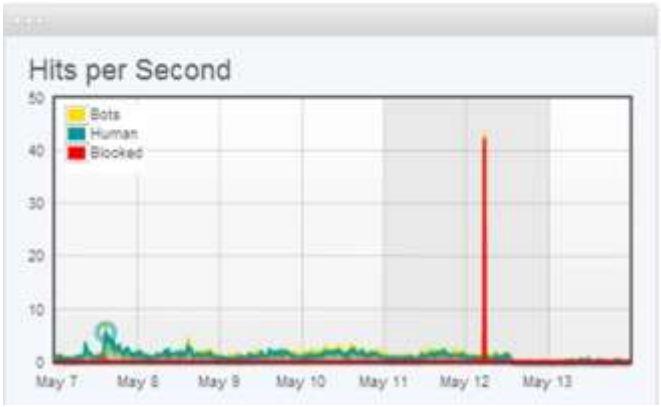
6.2 Man-in-the-middle attacks (MITM) pose a very serious threat when it comes to application security. If protection measures are not in place, these attacks are easy to execute, difficult to detect and reward the attackers with access to a plethora of sensitive user and business-related information. Given the level of damage these attacks can do, it becomes critical for business stakeholders to understand and identify their underlying vulnerabilities and implement all the preventive measures to keep their infrastructure safe and secure from these attacks**.**



6.3 To do so, a WAF typically relies on a large, and constantly updated, list of meticulously crafted signatures that allow it to surgically weed out malicious SQL queries. Usually, such a list holds signatures to address specific attack vectors and is regularly patched to introduce blocking rules for newly discovered vulnerabilities. Modern web application firewalls are also often integrated with other security solutions. From these, a WAF can receive additional information that further augments its security capabilities.

For example, a web application firewall that encounters a suspicious, but not outright malicious input may cross-verify it with IP data before deciding to block the request. It only blocks the input if the IP itself has a bad reputational history. We can use signature recognition, IP reputation, and other security methodologies to identify and block SQL injections, with a minimal number of false positives. The WAF's capabilities are augmented by Incap Rules—a custom security rule engine that enables granular customization of default security settings and the creation of additional case-specific security policies

6.4 Distributed DoS attacks are a genuine threat that cause serious damage to many Internet users. The losses being affected have increased from being merely annoying to actually being debilitating and disastrous for some users. There is every reason to believe that the rate and seriousness of DDoS attacks will increase. The current limited level of losses caused by DDoS is probably not due to successes in defending against them, difficulties in perpetrating the attacks, or lack of attractive targets to attack. Rather, the level of loss is related more to the motivations and desires of those who are perpetrating the attacks.



In the figure we can see how the attackers are hitting the host website in this way they will hit continuously and make the service enabled and cause huge losses to the organization so we can prevent them by reducing attack surface area, we should understand about the traffic by knowing the characteristics of normal traffic and abnormal traffic. by deploying firewalls to the sensitive information etc. and prevent them.

7. Conclusion

Cyberattacks are one of the most ambiguous factors which is quickly and constantly evolving that causes threat to computer or computer networks. Cyber criminals have introduced different hacking techniques and causes individual as well as business sectors more vulnerable to security problems. This paper outlined about the most common cyberattacks that are used by the attackers in order to compromise our critical information. These attacks cause a negative impact on the integrity, confidentiality and security of the system as well as the network. The major thing that we can do is to protect ourselves from attack is to understand about the possible threat and take required steps to safe guard the system and network. We can prevent them by deploying firewalls

and installing software's but we should take care about these attacks by continuously monitoring our network and we should also make sure that no one is trying to attack our server room physically also by installing some spywares etc. in this way we should take at most care to protect our network.

REFERENCES

1. Stiawan, D., Idris, M., Malik, R. F., Nurmaini, S., Alsharif, N., &Budiarto, R. (2019). Investigating brute force attack patterns in IoT network. Journal of Electrical and Computer Engineering, 2019.
2. Zhang, S., Xie, X., & Xu, Y. (2020). A brute-force black-box method to attack machine learning-based systems in cybersecurity. IEEE Access, 8, 128250-128263.
3. Park, J., Kim, J., Gupta, B. B., & Park, N. (2021). Network log-based SSH brute-force attack detection model. CMC-Computers Materials & Continua, 68(1), 887-901.
4. Faircloth, C., Hartzell, G., Callahan, N., &Bhunia, S. (2022, June). A Study on Brute Force Attack on T-Mobile Leading to SIM-Hijacking and Identity-Theft. In 2022 IEEE World AI IoT Congress (AIIoT) (pp. 501-507). IEEE.
5. Verma, R., Dhanda, N., & Nagar, V. (2022). Enhancing Security with In-Depth Analysis of Brute-Force Attack on Secure Hashing Algorithms. In Proceedings of Trends in Electronics and Health Informatics (pp. 513-522). Springer, Singapore.
6. M. Zviran and W. J. Haga, "Password security: an empirical study," Journal of Management Information Systems, vol. 15, pp. 161–185, 1999.
7. R. Morris and K. Thompson, "Password Security: A Case History," Commun. ACM, vol. 22, no. 11, pp. 594–597, Nov. 1979.
8. D. C. Feldmeier and P. R. Karn, "UNIX password security - ten years later," 9th Annual International Cryptology Conference on Advances in Cryptology, pp. 44-63, 2012.
9. D. Klein, "Foiling the cracker: A survey of, and improvements to, password security," Proceedings of the 2nd USENIX Security Workshop, pp. 5-14, 2011.
10. S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, "Does My Password Go Up to Eleven? The Impact of Password Meters on Password Selection," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2013, pp. 2379–
11. HashKiller.co.uk, [Online] Available: https://hashkiller.co.uk/ md5-decrypter.aspx, accessed December 2017.
12. M. L. Mazurek et al., "Measuring Password Guessability for an Entire University," ACM SIGSAC conference on Computer & Communications Security, 2013, pp. 173-186.
13. HashKiller.co.uk, [Online] Available: https://hashkiller.co.uk/ md5-decrypter.aspx, accessed December 2017.
14. M. M. Taha, "On password strength measurements: Password entropy and password quality," International Conf. on Computing, Electrical and Electronics Engineering,