Comparative Study of Traditional and Advanced Password Cracking Techniques used over the Internet

Aakanksha[1], Sanskriti Sharma[2*], Radhika Bisht[3] and Teesha Tiwari[3]

ABSTRACT

User authentication is becoming more and more crucial as internet technologies, social networks, and other related fields evolve quickly to protect user data. One of the popular techniques for achieving identification for authorized users and defense against intruders is password authentication. However, password security is facing great challenges. Over the past few years, numerous password-cracking techniques have been created, and security measures against password-cracking are constantly being developed. The process of guessing or retrieving a password from a stored place or through a data transmission system is known as password cracking. This paper is mainly to give a brief review of password-cracking techniques, key password-cracking technologies, password-cracking protection, and a comparison between the traditional and advanced password-cracking techniques. This paper will discuss what password cracking is, what to do if an attacker tries to log in to the system using a username and password combination, what steps to take if an attacker has access to how passwords are stored on the system, how to execute it when an attacker can somehow observe password entry, and how graphical passwords and graphical password cracks operate.

Passwords have been a target for hackers due to the significant benefits, and password cracking occurrences have increased. It's becoming essential to research password-cracking technology.

Keywords *: Network Security, Hacking, Cracking, Password, Password Protection, Password Cracking.*

1. Introduction

In today's world, the most important thing is the data and information that we possess. Moreover, the security of this data and information should be our priority. So, the protection of our data and information becomes a basic necessity. There are various ways to protect our data and information such as password authentication, two-step verification, one-time-password, biometrics, etc but

"Password" is the most commonly used technique of data and information security that is being used by most of us, nowadays.

Password can be understood as a "key" which can be numeric, alphabetic, or alphanumeric and may contain special characters too. It is used to identify the authenticated user who is the real owner of the data and information that is being retrieved. People generally keep passwords that are easy to memorize and thus, this helps in easy password cracking.

Password cracking is the technique that is used to decipher someone's password to have access to his or her private data and information. It refers to an online technique in which the attacker has gained access to the password hashes or database [6]. Password cracking can be done through application programs, software tools, hacking techniques, and password-guessing algorithms. Password cracking is, thus, a major threat to data and information that belongs to a person.

There are various methodologies to crack passwords, which have evolved in recent times and are being discussed in a further section. Some of the commonly used password-cracking techniques are – Dictionary search, Phishing, Rainbow attacks, etc. Across the world, there are serious password-leakage incidents taking place which are of great danger to people and their private information [8].

A dictionary attack is one of the most popular techniques employed to crack passwords. It is done using automated tools where every single, possible word in the dictionary is tried as a password. It is a time-consuming process to crack passwords & hence cannot be employed to crack passwords that are valid for a short period, such as one-time passwords.

[1] *Department of Computer Science, SRCASW, University of Delhi.*
[2] *Department of Chemistry, SRCASW, University of Delhi.*
[3] *Department of Instrumentation, SRCASW, University of Delhi.*
* *Corresponding Author ✉ sanskriti.sharma2812@gmail.com*

Received: 22 October, 2023
Available online: 31 December, 2023

Thus, we all should be very cautious while creating our passwords. It is advisable not to share our passwords or OTPs with anyone. We should not keep passwords that are easy to predict. It is analyzed that passwords and personal information secured by them are correlated, hence it automatically becomes important to avoid sharing your personal information with anyone [3]. We should be alert while dealing with secured applications in public places.

This paper discusses the various aspects of "Password Cracking". It covers the evolution of the password-cracking technique, its various methods, its implementation and the various ways to be protected against it. It is a review of the research that has been done so far in the field of "Password Cracking Methodologies".

2. Background and Related Work

A secret word (made up of a string of characters) called a password is used to establish an identity to access a particular resource. The word "password" is made up of the two words "pass" and "word," and refers to a word that serves as a secret word (or pass) for authentication. Since ancient times, people have used passwords. Soldiers in the past used passwords as a code word to access a highly restricted sector of a kingdom.

In the current era, sometimes known as the digital age, people use a combination of usernames and passwords to authenticate themselves while logging into digital devices. Passwords are used to secure all types of digital devices, including computers, smartphones, gaming consoles, PDAs, and more. A computer user uses passwords for a variety of things, including accessing mail accounts, databases, networks, websites, and apps. This new era of the digital revolution has brought about various security threats in the realm of the Information and Communication Technology sector. The present scenario can only be corrected when one has adequate knowledge regarding password cracking tools, their evolution, and their advancement.

Now that we are aware, passwords are used for security purposes, and breaches will still happen no matter how secure things are. Passwords are often recovered through the method of "cracking," which involves accessing computer devices' stored data. Password cracking is used, maliciously, to get access to a computer system even if its intended application is to recover forgotten passwords. To crack a password, the attacker must go through two unique stages. The initial step involves dumping the password hashes, and the second stage requires attempting to crack the hashes that have been collected. In addition to this technique, passwords can also be cracked by guessing them, using malicious tools like keyloggers, engaging in phishing attacks, utilizing social engineering, skipping diving, shoulder surfing, etc.

We are now entering a historical flashback of password cracking, showing how password hashes were broken ten years ago. Some well-known programs, like Cain and Abel and JohnTheRipper; Cain and Abel password-cracking techniques have a specialty in using several attacks to get the password [11]. Similarly, JohnTheRipper uses two distinct algorithms to crack passwords using the Message Passing Interface [12]. This software makes use of the CPU cores to decode the hashes into plaintext. Therefore, if the password is strong and complicated (a password that contains alphanumeric, special characters), it will take days or years to decode the hash and reveal the plaintext. However, we no longer experience the type of situation where the password is lost after the system has been functioning for several months. The cracking times for certain common passwords are getting too quick thanks to advanced approaches. These include loading rainbow tables onto incredibly fast solid-state drives (SSDs) and using graphical processing units (GPUs) on video cards. Such GPU-supported software as Hashcat, Rainbow Crack, Cryptohaze Multiforcer, etc. makes use of the GPU cores to decipher hashes.

In this section, we learn that there are two elements—the CPU and the GPU – that are crucial to the process of breaking any hash. We will study the CPU and GPU in the part that follows, as well as how the GPU operates more quickly than the CPU.

Why GPU and Not CPU?

All program instructions are carried out by the CPU, or central processing unit. The graphical processing unit, or GPU, is designed to lighten the load on the CPU by taking care of all the complex computations required to display the final result on the monitor. A computer's GPU is referred to as its soul, and its CPU is thought of as its brain.

The integrated chips in most PCs produce the display images on the monitor. Only simple visuals, such as those found in Microsoft Office, low-resolution games, and films, are rendered by Intel's integrated graphics. The GPU's primary purpose when it was first created was to produce 2D (two-dimensional) images and speed up the generation of windows in graphical interface mode. But as technology advanced, a 3D (three-dimensional) era emerged that necessitated faster visual rendering. There has been an increase in GPU acceleration that is quicker and more task-specific. Hardware-wise, the GPU and CPU are comparable but not identical. Architecture-wise, the CPU only has a few cores / numerous cores with a lot of cache memory, and it can manage a small number of software threads concurrently. A GPU, on the other hand, has thousands of cores and can manage threads at once. Some software can be 100 times faster when running on a GPU with 100 or more cores than on a CPU alone. With hundreds or even thousands of cores, the GPU uses significant parallelism to achieve excellent performance. Pipelining and shared instruction decoding make this possible. A GPU like the Radeon HD 5970 can process

3200 32-bit instructions per clock as opposed to a CPU core's four 32-bit instructions per cycle.

GPUs are extremely specialized in number crunching, which graphics processing sorely needs since it entails millions, if not billions, of computations per second. This is how GPUs and CPUs differ from one another. The use of multiple GPUs is also possible, much like the dual-core CPUs that are now on the market. The maker of the graphic card determines the core count. While AMD graphics solutions often include more cores to boost processing power, Nvidia graphics solutions typically pack more power into fewer chips. The GTX Titan, a new graphics card from Nvidia, contains 2688 cores.

After much discussion, we now understand why the GPU is used to decipher passwords.

3. Motivation

The increasing threats to online security against privacy breaches and theft; have made the understanding of password cracking techniques a necessity. This issue of lack of digital awareness among people is to be mitigated through the general awakening of society in the arenas of digital security and confidentiality. An understanding of traditional and advanced password-cracking techniques helps in getting the approach to have a strong authentication factor for our applications so that their security breach is prevented. New techniques like deep fakes, generative artificial intelligence, and others have created a strong requirement among people to know about hacking and cracking methodologies very well.

4. Password Cracking techniques

Evolution: Password protection has been used as a tool to protect vulnerable information and data, from older times. Fernando Corbato was the person who presented the idea of passwords at the Massachusetts Institute of Technology in the year 1960. Earlier passwords were only used by authorities in the field of research and academic circles, but with advancements in technology the use of computers became general and thus, the computers were susceptible to threats of piracy and stealing. Hence, passwords have been used widely by people to protect their important information and avoid hacking of their devices. But, hackers too developed advanced techniques to crack passwords to peep into the systems of users and steal their information. Nowadays, many firms such as Microsoft, Wwwhack, etc have developed good password recovery software for the files of applications like MS Excel, MS Word, ZIP, etc, to protect the information stored in them against efficient password cracking [5]. Thus, new technology has curated the need to develop strong password-shielding mechanisms. So, to get an idea of the old and new password-cracking techniques we have discussed some of the most popular algorithms that were mainly used in the 20th century, to execute hacking and cracking of devices along with the most recent password-cracking techniques used in today's digital arena.

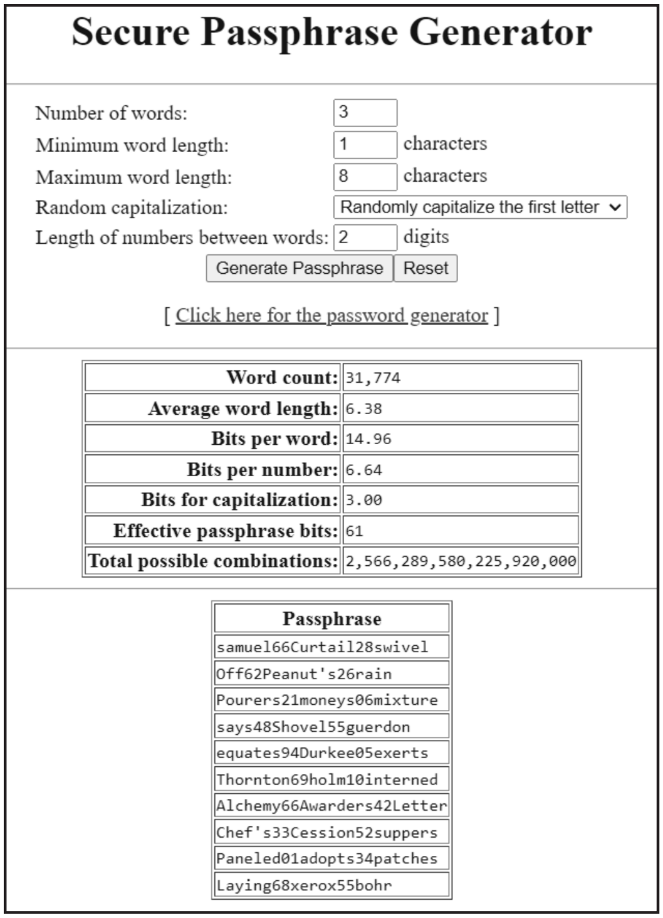
5. Traditional Password-Cracking Techniques

5.1 UNIX Password System

UNIX Password Systems were very popular at the time of evolution of the password-cracking techniques. This methodology was used in the educational environment where there was an increased concentration of hackers. In a UNIX system of password protection, the encryption module used DES (Data Encryption Standard) algorithm, 25 times in a row. The flow of encryption takes place in several rounds. The first DES round uses 64, 0-bits and encrypts them with the user's password by applying permutations. The number of possible permutations is 4096 and is chosen randomly by the hacker for each user. The same process is repeated until the password is hacked and the information is taken off the system. Thus, the UNIX password system was an easy password-cracking technique and gained popularity due to its easy applicability and versatility.

5.2 Passphrase Cracker

A Passphrase was used instead of one-word passwords to ensure more security of data. Passphrases are mainly



Secure Passphrase Generator

Number of words: 3

Minimum word length: 1 characters

Maximum word length: 8 characters

Random capitalization: Randomly capitalize the first letter

Length of numbers between words: 2 digits

Word count:	31,774
Average word length:	6.38
Bits per word:	14.96
Bits per number:	6.64
Bits for capitalization:	3.00
Effective passphrase bits:	61
Total possible combinations:	2,566,289,580,225,920,000

Passphrase
samuel66Curtail28swivel
Off62Peanut's26rain
Pourers21moneys06mixture
says48Shovel55guerdon
equates94Durkee05exerts
Thornton69holm10interned
Alchemy66Awarders42Letter
Chef's33Cession52suppers
Paneled01adopts34patches
Laying68xerox55bohr

Figure 1. *An example of a Passphrase Generator.*
(Source: https://untroubled.org/pwgen/ppgen.cgi)

multiple-word phrases using letters, symbols, and spaces along with symbols that have very intricate keys to crack. Passphrases are even used in advanced password-cracking methodologies. These passwords were nearly impossible to crack, easy to memorize for the users, and were supported on all operating systems to ensure a fully secure online experience.

Passphrase Crackers were also designed to crack the passphrases of devices and applications to steal information from hackers. Their algorithm was similar to that of the passphrase generator and gave a combination of passphrases that were hit and tried on the devices and applications until the correct passphrase was matched.

However, passphrases were more secure than other traditional password protection methodologies.

5.3 Stealing

Stealing is basically using fraudulent practices in order to gain access to passwords. In this, the hacker may look for the password in the person's office, may shoulder surf, sniff or use friendly tones so as to have unauthorized access to the victim's password. Shoulder surfing includes the practice of dressing up differently as the hacker in the form of a peon, technician, or engineer in order to peep into the office or system of the user. Sometimes, the hacker installs malware in the central system; this malware is shared with other computers through a network; the malware makes a backup of all the activities taking place on the system and in this way, it records the login details of the user which is accessed by the hacker at the end [1]. The major password-cracking methodologies involved in stealing other than Shoulder-Surfing Attacks are Eavesdropping Attacks and Phishing [13].

5.4 Defrauding

Defrauding mainly refers to the use of social engineering and phishing in order to have access to the password of the victim. In social engineering, the hacker pretends to be an IT professional who calls and gradually establishes friendly communication. He then persuades the user to give out his bank details or network access and thus gathers sensitive information [1].

In phishing, emails are sent to the user which is actually fraud emails containing links that are directed to fake, malicious websites; if the receiver, by mistake clicks on such links he/she may end up directing all their network credentials or even device information onto the corrupt website.

5.5 Algorithm Analysis

Algorithm analysis uses cryptanalytic attacks which are used in the decryption of ciphertext too. The ciphertext or the encrypted data is decrypted by exploiting the characteristics of algorithms to deduce a plaintext-ciphertext pair or the key of the algorithm.

5.6 Fully Guessing

This method uses the dictionary attack, brute-force attack, or a hybrid of the dictionary or the brute-force attack. In the dictionary attack, the hacker searches a large dictionary of possible passwords to gain access to the user's network. Encryption is applied to match the password in the password-containing file [1].

In a brute-force attack, the hacker guesses the password and tries this approach until he finds the password that works. In the brute-force attack, unlike in a dictionary attack, where only meaningful words are used as passwords; the passwords can be alphanumeric and collections of letters, numbers, special characters, symbols, etc.

5.7 Probabilistic Password Cracker

In this method of password cracking the hackers use probabilistic or common context-free grammar to find out how the guessed password was somewhat like the original password of the user [4]. The idea behind this method was that the probability of guessing a password was different each time a new password is guessed. FGPA implementation requires four-password derived encryption key generation units that operate at a frequency of say, 150 MHz and process approximately, 560 passwords per second [15].

Let's ponder on some advanced password-cracking techniques that have more sophisticated algorithms and are used by high-end hackers and crackers.

6. Advanced Password-Cracking Techniques

6.1 FPGA (Field Programmable Gate Arrays)

These are versatile silicon chips that provide very high speed to operations being executed onto a computer system. FGPAs use less power and run at very low clock speeds. FGPAs are used in password cracking to generate the permutations or combinations of passwords at a much faster speed with minimal power usage and at the same time prevent the time of notice by the victim.

6.2 JohnTheRipper

JohnTheRipper is a password-cracking program by Openwall. It is very fast and is gaining tremendous popularity nowadays. Earlier it was used to crack UNIX Passwords but nowadays this application is also being used to crack Windows LM hashes [2].

6.3 Rainbow Crack

In the Rainbow Crack, password-cracking mechanism, rainbow tables are used to find the password [2]. In the initial step, rainbow chains are generated which are stored in a special format in the binary rainbow table file, then these stored passwords are matched with the password file and if it matches then the password is again matched using a lookup method. In an improved rainbow attack combination of a dictionary generator and rainbow, the table approach is brought into use for more efficient and smart cracking of long and complicated passwords [10]. An important disadvantage of this method is that it takes up a large amount of space in the computer system's memory.

6.4 Cain and Abel

It is a Windows password-cracking tool. It is known for its versatility. Moreover, this technique also acts as a sniffer on the network. The main types of techniques that it uses to crack passwords are – Brute Force Attacks, Cryptanalysis attacks, etc.

6.5 Hashcat

Hashcat is an open-source cracking tool for Windows, OSX, and Linux. It uses the Dictionary as well as the Brute-force attack for generating passwords and performs the cracking process within a very small amount of time. Hashcat calculates 'keyspace' which corresponds with the actual password in 85% of cases of password-cracking [14].

7. Results and Discussion

In this section, we are emphasizing the various types of password-cracking techniques that have evolved till now in the arena of information security. From traditional password-cracking mechanisms to the advanced hijacking of systems, the most important password-cracking mechanisms have been discussed below in detail. Broadly, password-cracking techniques have been classified into two parts, which are shown below. Further, they have been discussed in detail. The traditional password-cracking techniques were employed in decoding the passwords and authorizations of older software and less protected applications. The usability of advanced password-cracking techniques is in modern applications that use intricate software and complex algorithms that are based on microsecond evaluation. Moreover, traditional password-cracking techniques have been found to evolve from the ideas used to send messages between ancient monarchs and their diplomats, as in the case of the Caesar Cipher technique. Modern password-cracking methodologies have the basis of newer techniques like the generative artificial technique which is commonly used nowadays for recognition and resemblance.

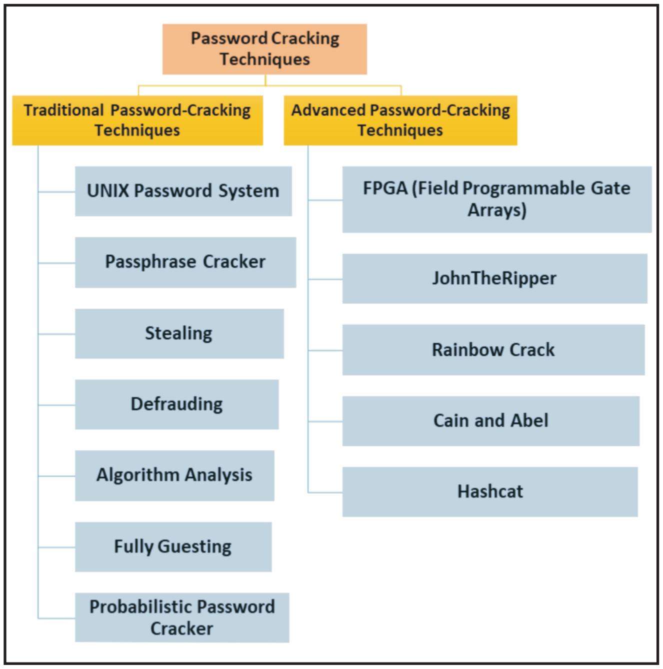

Password Cracking Techniques
Traditional Password-Cracking Techniques
Advanced Password-Cracking Techniques
UNIX Password System
Passphrase Cracker
Stealing
Defrauding
Algorithm Analysis
Fully Guesting
Probabilistic Password Cracker
FPGA (Field Programmable Gate Arrays)
JohnTheRipper
Rainbow Crack
Cain and Abel
Hashcat

Figure 2 : *Classification of Password-Cracking Techniques.*

The table depicts the comparison between traditional password-cracking techniques and advanced ones on various parameters.

Table 1 : *A comparative study of traditional and advanced password cracking techniques.*

Parameters of comparison	Traditional Password-Cracking Techniques	Advanced Password-Cracking Techniques
Speed of password generation	Slow	Fast
Power and storage usage	Low power consumption and high storage consumption.	High power consumption and low storage consumption.
Manpower	High	Negligible
Ability to generate correct password	Low	High

A comparative study of the traditional and advanced password-cracking techniques underlines the methodology that should be adopted while using any protection methodology for your system and your device. The speed of pattern recognition and the efficiency of results are two important parameters that can be employed in deciding on a password-cracking mechanism.

8. Conclusion and Future Scope

In the contemporary world, the password is a means to secure someone's personal information. Password is a combination of alphabets, numbers, and special characters to authorize a user to access any secured information. The password remains the most widely used method to ensure authentication [1]. Passwords are required to authorize access to mail accounts, banking websites or apps, databases, networks, and other secured websites and apps.

In the previous sections, we discussed the history of password cracking and the various techniques used by hackers to break into our systems. Password cracking is an actual threat and all our information is at risk nowadays. The most typical way to crack passwords is to get a file containing user-hashed passwords and then run a cracker against the file to try to get matches for all the hashes [2].

Through the years, password cracking has become even easier with the help of artificial intelligence. So, our password is always at risk because of the artificial intelligence environment. To avoid easy cracking of our passwords, there are several measures that we need to take care of such as using longer passwords, avoiding using personal information while creating passwords, using different passwords for different accounts, and never sharing your passwords with anyone. Your password should be at least 8 characters long, must contain at least one letter and at least one digit, and must contain at least one special character [7]. Using these measures can minimize the threat of password cracking; however, our passwords are not fully safe all the time. It is a myth that if your password is strong, your data and information are safe but, hackers can crack any password usually, it takes much more time if the password is strong. Due to advancements in technology, routers and some other computing devices have also been password-protected against brute-force attacks. As these routers control the whole network thus, they need to be protected against any threat [9]. Thus, devices are also protected through strong passwords, also as a countermeasure, we should keep changing our passwords from time to time and should remember that good and strong passwords are very vital for system and information security, but, due to advanced techniques, hackers enter a system even without using passwords, thus, having a strong password is not solely adequate to resolve the risk of password cracking.

References

1. Lifeng Han, "Password Cracking and Countermeasures in Computer Security: A Survey", **2023**. https://arxiv.org/pdf/1411.7803
2. John A. Chester, "Analysis of Password Cracking Methods & Applications", *Honours Research Projects*, Vol. **7**, **2015.**
3. Shen He, Jun Fu, Cancan Chen, Zhihui Guo, "Research on Password Cracking Technology Based on Improved Transformer", *Journal of Physics Conference Series*, **2020**. DOI:10.1088/1742-6596/1631/1/012161.
4. Shiva Houshmand Yazdi, "Analyzing Password Strength & Efficient Password Cracking", *Florida State University Libraries*, **2011**.
5. Hsein-Cheng Chou, Hung-Chang Lee, Hwan-Jeu Yu, Fei-Pei Lai, Kuo-Hsuan Huang, Chin-Wen Hsueh, "Password Cracking Based on Learned Patterns from Disclosed Passwords", *International Journal of Innovative Computing, Information and Control*, Vol. **9**, **2013**.
6. Eric Conrad, Seth Misenar, Joshua Feldman, "CISSP Study Guide", **2010**.
7. Yinqian Zhang, Fabian Monrose, Michael K. Reiter, "The Security of Modern Password Expiration: An Analysis Framework and Empirical Analysis."
8. Shouling Ji, Shukun Yang, Xin Hu, Weili Han, Zhigong Li, Raheem Beyah, "Zero-Sun Password Cracking Game: A Large-Scale Empirical Study on the Crackability, Correlation, and Security of Passwords", *IEEE Transactions on Dependable and Secure Computing,* Vol. **14**, **2017**.
9. Mohammed Farik, ABM Shawkat Ali, "Algorithm to Ensure and Enforce Brute-force Attack-Resilient Password in Routers", *International Journal of Scientific and Technology Research*, Vol. **4**, **2015**.
10. Lijun Zhang, Cheng Tan, Fei Yu, "An Improved Rainbow Table Attack for Long Passwords", *International Congress of Information and Communication Technology*, **2017**.
11. Seung Hyun Kim, Dimitry Vasin, "Cain and Abel Report", *CS Toronto*.
12. Edward R Skyes, "MPI Enhancements in JohnTheRipper", *Journal of Physics: Conference Series*, **2010**.
13. Venkadesh S, Palanivel Kuppusamy, "A Survey on Password Stealing Attacks and Its Protecting Mechanism", *International Journal of Engineering Trends and Technology*, **2015**.
14. Radek Hranicky, Lukas Zobal, Ondrej Rysavy, Dusan Kolar, "Distributed Password cracking with BONIC and Hashcat", **2019**.
15. Yoginder S. Dandass, "Using FPGAs to Parallelize Dictionary Attacks for Password Cracking", *Hawaii International Conference on System Sciences*, **2008**.

❖ ❖ ❖