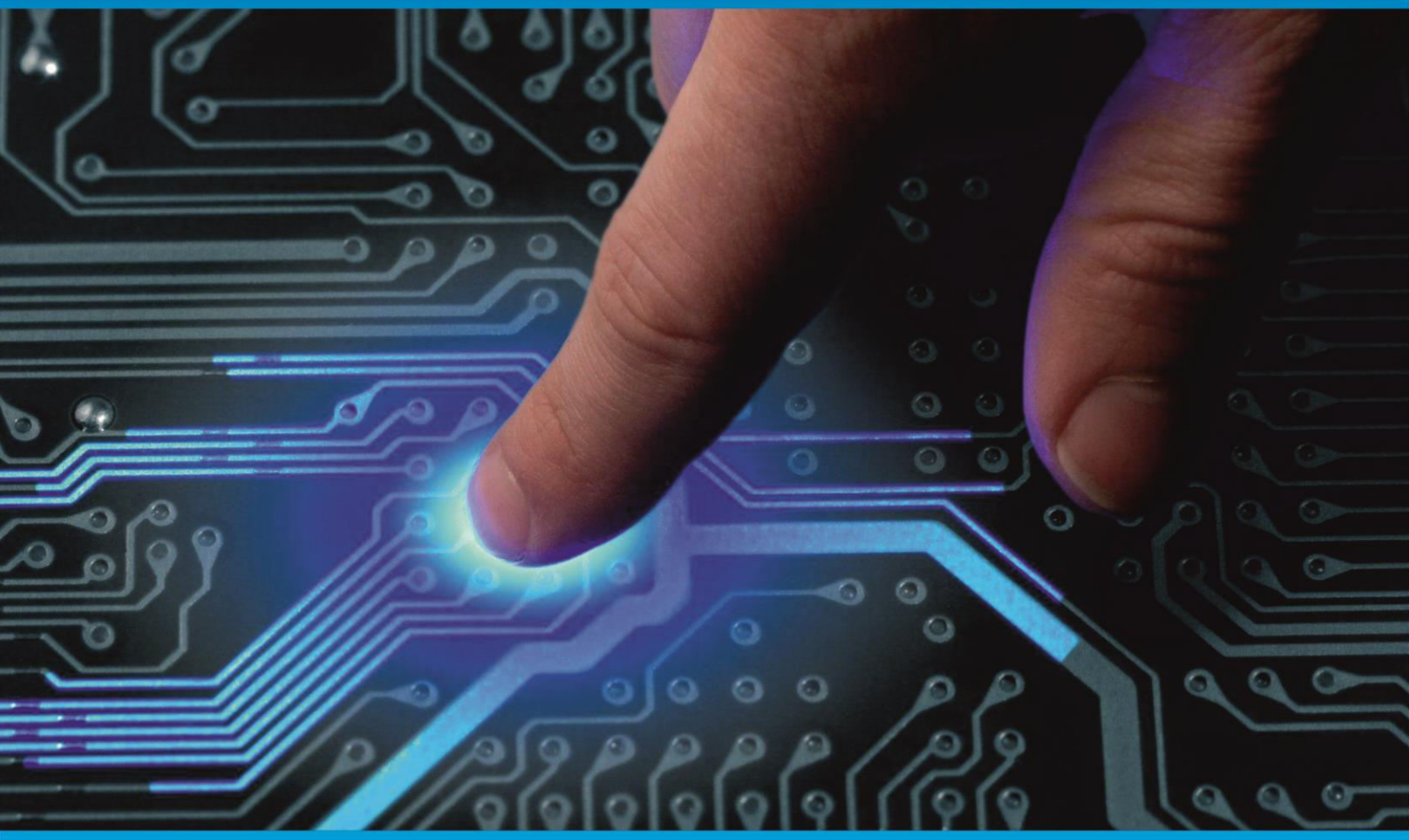
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903130|

Review on Password Paradigm

Mayuri Hanumant Chavan[1], Dr.Vaishali Sanvikar[2]

Student , Department of M.C.A, P.E.S.'s Modern College of Engineering Pune, Maharashtra, India [1]

Head of the Department, Department of M.C.A, P.E.S.'s Modern College of Engineering Pune, Maharashtra, India [2]

ABSTRACT: The Internet is that the most integral a part of our lifestyle and therefore the people that manage their work with internet-like bank transactions, online shopping also are constantly growing. The websites which give these services should be an authenticated one i.e., they ought to allow the username and password with a reliable service. . Normally, people maintain an equivalent username and password for the websites they use. this sort of behavior can cause the hackers to hack the password and may easily retrieve the users' personal information within a couple of seconds. Hash functions are wont to build secure password data .Some encoding techniques also are used for password protection.

KEYWORDS: Brute force , Dictionary, Key Loggers , Security , Keystroke

I. INTRODUCTION

A password is information related to an entity that confirms a private identity. A password could also be a secret which is simply known to you. A password provides access to a service for a selected user and is employed to verify the identity of the user. The system is usually your pc, your email account, your online bank account or any web account. Your passwords are often stolen and guessed someone could impersonate you online, can also steal money from your online bank account , send emails in your name or change files on your computer to call just a couple of of the possible outcomes.. Password guessing is formed easier by revealing the private information and having related passwords. it's easily detected and stopped. presume employing a dictionary would save time. Such passwords are usually weak. Surveys depict that the bulk of the users keep their relations details, personal information,their likings, famous sports teams etc. One can make the thanks to others computers through some application programs and by sending files which open their ports. Thus, gain access to the victim's data and knowledge . Password guessing isn't sound and complicated technique to crack passwords because there's no surety that passwords are becoming to be cracked.

II. LITERATURE SURVEY

There are variety of passwords attacks and few of them are described here, in order that a person can understand and remember of unauthorized access or passwords attacks. Some contributors have surveyed authentication philosophy, attacks and graphical password methods. the aim of this research is to spotlight the benefits and drawbacks of various secure authentication methods and supply awareness to persons about password attacks and suitability of authentication methods during a particular scenario.

2.1Authentication Methods Based on Password [2]

Conventional Password Scheme: during this scheme the user enters or logs in into the system through his username and password. The systemfirst authenticates the user from the user database and on the thought of authentication of the user then grants the access to the system.

Keystroke Dynamics: The Keystroke Dynamics stores the next time patterns of the user alongside the normal password.

- Time between the key pressed and release
- Time between the 2 keys pressed.

Click Patterns: In this type of password scheme, the user is provided with a click pad on the screen. The click pad can contain different color grids or it is often the mixture of various symbols. The user can mislead the attacker by using the press pattern as a password.

Authentication Panel: In these password schemes rather than pressing the exact button for password, the user is prompted to pick the situation of the password words from the given panel. It provides resistance against brute force,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903130|

dictionary, shouldering and video attacks. It does not require extra hardware and it is fast.

Virtual Password: This Novel password scheme offers secure user's password in on-line environments .It can provide protection against different online attacks. As phishing and password file compromise attacks.

III. PASSWORD MEANING

3.1Composition [4]

A password is a secret word or string of characters that is used for authentication. Password security basically every security system is based on password .

A password…

- Is a combination of string of letters, numbers, and/or special characters
- Is the primary authentication and authorization method
- Should be stored encrypted
- It is a strong word or phrase
- It can also be easily get cracked or hacked
- Hash functions and Rainbow table are used
- Algorithms can be used to secure the authentication.
- Passwords are commonly used with your username.

IV. PASSWORD MEANING

Password attack means a 3rd party trying to realize access to your systems by cracking a user's password. This sorts of attack doesn't usually require any sort of malicious code or software to run on the system. there's software that attackers use to undertake and crack your password, but this software is usually run on their own system.

4.1 Brute force Attack [5][6]: 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.

Prevention techniques for stopping Brute Force Attacks:

1. Account Lockouts After Failed Attempts
2. Make the Root User Inaccessible via SSH
3. Use CAPTCHA
4. Limit Logins to a Specified IP Address or Range
5. Use Unique Login URLs

4.2. Dictionary Attacks: A dictionary attack is predicated on trying all the strings during a pre-arranged listing. However, now there are much larger lists available on the open Internet that contain hundreds of millions of passwords recovered .There is also cracking software like brutus and John the ripper.

Prevention techniques for stopping Dictionary attacks

- Set up multi-factor authentication where possible.
- Limit the amount of attempts allowed within a given period of your time.
- Force account resets after a particular number of failed attempts.
- Include captchas

4.3 Phishing: Phishing is a type of attack including login credentials and credit card numbers. It occurs when a user tries to open an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which may cause the installation of malware and therefore the system as a part of or the revealing of sensitive information.

Prevention techniques for stopping Phishing:

• You can use Two-factor authentication (2FA) to stop phishing attacks. It is an additional verification layer. 2FA relies on users having two things: something they know, like a password and username, and something they need like their smartphones. Even when employees are compromised, 2FA prevents the utilization of their compromised credentials,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903130|

since these alone are insufficient to realize entry.
• Organizations should create strict password management policies. for example, employees should use mostly one time passwords.
• On various college campuses we can use some methods to stop phishing attacks.

4.4 Man within the Middle Attack: In cryptography and PC security, a man-in-the-middle attack (MITM) is an attack where the attacker furtively transfers and perhaps changes the correspondence between two parties.A man within the middle (MITM) attack may be a general term for when a culprit positions himself during a discussion between a client and an application; either to concentrate stealthily or to imitate one among the parties, making it show up as if a standard trade of data is ongoing.The data which can be stolen is for example, login certifications, account points of interest and charge card numbers.

Prevention techniques for stopping Man in the Middle Attacks

•Educate people to stop cyber-attacks, cyber threats and what they should to avoid compromising the security of your organization.
•Use VPNs (Virtual Private Network) in order to ensure the secure connections.
• You can use secure encryption techniques
•Make a habit of regularly updating passwords of your networks and devices.
•Try to use secure browsers and the latest version of it.
•Get browser plugins like Force TLS of HTTPS Everywhere to secure the sensitive online transactions.
•Separate your Wi-Fi network.

V. FORMULAE FOR STRONG PASSWORDS

The following points should be taken into considerations when selecting passwords.

- The passwords should not be based on common words used .
- If a password has to be picked from social words, it should be broken down into pieces and digits and special characters should be inserted in between and the end.
- If numbers are used in the passwords, the flow should not be in ascending order nor in descending order.
- Passwords should not represent years and birthdays.
- Special characters like "_" and "-" should be avoided as it has been used excessively and the hackers are aware of this fact.
- Passwords should not be contain family members name
- Passwords selection should be planned and not chosen at a particular instant during registration. This helps in avoiding selecting passwords based on immediate feelings.
- While creating the passwords try to use some phrases.

VI. CONCLUSION

Password is the key which only you know and it acts like a defense mechanism in various sites. We hereby attempt to aware the mass about a number of the possible threats to passwords and measures to stop them from being hacked or stolen. Password cracking software is growing these days. One should make a habit of using strong passwords which reduce the probability of password being hacked and attacked.
Passwords should never be used more than once or twice. Hopefully this paper will enlighten your views and supply some grip in acquiring more information about particular thorough information. There are several ways by which the password can be attacked, only awareness and precautions can help from being hacked or attacked. Through this several things are concluded as before adopting any password or authentication method, the user must know the password attack and then the user should apply an appropriate solution. The user should apply the authentication method according to scenario because some of the methods are applicable at standalone system and some are applicable at online environments .Although several schemes described here provide protection against dictionary attacks, brute force attacks, video recording attacks, spyware, phishing etc. but in order to secure system.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903130|

REFERENCES

1. https://krazytech.com/technical-papers/password-paradigms
2. A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication MudassarRaza, Muhammad Iqbal, Muhammad Sharif and WaqasHaiderComsats Institute of Information Technology, WahCantt., 47040, Pakistan
3. https://www.academia.edu/12257531/Design_and_Development_of_Two_Factor_Hash_Based_Authentication_Framework
4. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=358994b2-7e53-4f96-b4e8-926ea2d91b2a&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
5. https://en.wikipedia.org/wiki/Brute-force_attack
6. https://www.kaspersky.com/resource-center/definitions/brute-force-attack
7. https://www.imperva.com/learn/application-security/phishing-attack-scam/
8. https://www.researchgate.net/publication/221005667_A_man-in-the-middle_attack_on_UMTS

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details