RESEARCHERID
THOMSON REUTERS
[ICITAIC-2019]
ISSN 2348 – 8034
Impact Factor- 5.070
GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

PROTECTING PASSWORDS USING C++

A.Srigreeshma,D. Shreeprada, E. Sravya, Ms.P R Anisha, Dr.B Ramana Murthy and Mr.C Kishor Reddy
Stanley College of Engineering and Technology for Women, Chapel Road, Abids, Hyderabad, 500001.

ABSTRACT
Nowadays people are spending most of their time on social media .Each person maintains several accounts for eg: facebook, instagram, whatsapp, googlepay, gmail accounts etc. It is difficult to remember all the passwords of such accounts and we cannot use the same password to all the accounts because of risk factor. Therefore we have planned to store all the passwords of these accounts in a a file and to secure this file with a password. We can open this file and obtain the required password .The reason that we have taken this project is to make it easy to store and retrieve the passwords in a simple and secured manner.

Keywords: *C++,user name , password, Files.*

1. INTRODUCTION
Combination of user ID and The password is used for authentication ,is one of the best authentication, In this authentication process there are two steps

1 .User ID and Password:

Firstly user is created . Then password is selected. The password should be kept secret and should not share with other persons

2. Log-on:

Users should enter both their user IDs and passwords during login process. The system checks whether the given data is matched or not If it matches user can access it otherwise user will not be allowed to access

Instead of remembering all the user IDs and passwords ,we can store them in a single file. Whenever you want some data like any password or user ID you can access the file and can obtain the required data. So ,to keep this file safe we need to lock it with a password .Such that if you want to access /open the file you have to enter the correct password .So ,the password should not be stored because most of your passwords of others accounts are stored in it

Passwords should be strong but not weak

Characteristics of weak passwords:

1 .Passwords less than fifteen characters

2. Passwords available in dictionary

3. Passwords such as names of family ,pets.

4. Passwords like birthdays, address, phone no etc

5. Passwords with numbers/words, patterns like aabb, 1122 etc

ISSN 2348 – 8034
Impact Factor- 5.070

2. LITERATURE SURVEY

Zviran and Haga conducted a survey on computer users. They came to know that 24.91 of the respondents had 6 characters in their passwords and 80.1%passwords consisted of only alphabetic characteristics

They finally observed the following:

1. Passwords memorizability is affected by password selection methods

2. Changing passwords frequently saves your account from hacking

3 .Best passwords is it must contain alphabets, numbers, special characters, minimum length of 8

Adams and Sassc observed that:

1 .Passwords must contain upper and lower case characters

2 .Passwords contain numbers, symbols for example:12pinky@

3 .Passwords should not be based on personal information such as names of family, telephone no etc.

4. Password must be unique and easy to memorize

Secure data storage depends on how you create and use the passwords that are needed to access your data. Passwords should be difficult to determine and also protected carefully .They should be never shared, never written any where .Princeton University's OIT is an excellent resource for information on creating and managing passwords

3. PASSWORD PROTECTION

1. Avoid reusing passwords

2. Same passwords for multiple accounts should be avoided

3. Don't use automatic logon functionality

4. Strong passwords should be used

4. TIPS TO PROTECT DATA STORED IN YOUR COMPUTER

1. Encrypt data

2. Backup your data

3. Anti-malware protection is must

4. Make your old computer's hard drives unreadable

5.Install operating system updates

6. Automate your software updates

7.Secure your wireless network at your home orat work

5. TIPS TO PROTECT DATA STORED IN YOUR MOBILE

1. Check app privacy settings

2. Lock the mobile

ISSN 2348 – 8034
Impact Factor- 5.070

3. Backup your mobile device data

4. Disable automatic uploading

5 .Disable blue tooth when it is not under use

6. Get antivirus

7. Check push notifications

8 . Don't install unnecessary apps

9. Be careful during online transaction in public

6. ALGORITHM

1.Create a file

2. Open the file

3. First store the user ID and passwords of one account in a file

4. Then append other details to it

5. Now lock the entire file

6. The password must be :

a. 8 characters long

b. Should contain alphabets ,numbers

c. Should be unique

d. Contains upper and lower case

e. Should not be based on family names or pet names

f. Should be easy to memorize

7. Close the file

8. If you want to access the file

a. Open the file

b. Enter the password

c. If the password is matched then you can access it

d. If it doesn't match it gives a notification to try again

9. If you access the file the details are displayed

10.Suppose in this if we have given any three accounts details say email, facebook, googlepay

ISSN 2348 – 8034
Impact Factor- 5.070

11. When you access it then it displays:

1. Email

2. Facebook

3.Googlepay

12. If you select 1 that is Email then

Username and password of that particular account is displayed. Similarly you can get your required data

13.Close the file whenever your work is done

7. ADVANTAGES

1.Only you can access the files

2.No need to remember all the passwords or user IDs ,Just one password is enough to remember

3.Safe and secure

4.Easy to manage

5.Easy to access

6. Simple to use

7. Generate random passwords

8. Login to accounts is simple

9 .You can change the passwords easily

10. Can be used for longer time

11..Passwords are kept in one safe place

12. It allows generating robust passwords

13. It is of low cost

14. It is widely used

15. Reliable

8. DISADVANTAGES

If your password is leaked then all the passwords that are stored in the file will be leaked and may results in is hacking all your accounts

9. FUTURE BENEFITS

Passwords have been around for decades now, and they aren't going away any time soon.

And yet, password security best practices have been ignored by many. Too many people and companies are careless with password management, even though they know that a single password in the wrong hands can lead to disastrous consequences.

ISSN 2348 – 8034
Impact Factor- 5.070

If you're overwhelmed by the task of managing dozens, even hundreds, of personal or business passwords securely, or you've never had to deal with the aftermath of a hack, you may be tempted to keep your head in the sand and hope for the best. This is your worst possible option.

As recently as mid-2016 Pew Research Center reported that most Americans keep track of their online password by memorizing them or writing them down. And if they do this with personal passwords, you can be sure that some of this behavior finds its way into your office environment where the security risks are amplified.
No surprise again, 123456—possibly the worst password ever—continues to be the most used password for the 5th year in a row.
Other bad password security practices from the 1990s are also alive and well:

- Companies still add computers to their network without changing the default, out-of-the-box password.
- Employees still email passwords to one another.
- Organizations still store passwords in "password protected" Excel spreadsheets (see why that's a lousy idea), and employees still write sensitive passwords on sticky notes and paste them on their monitors or under their keyboard.
- People still choose the worst passwords ever—Wikipedia publishes SplashData's "List of the most Common Passwords" every year, and the old favorites are always pretty much the same.
- **Has anything changed in password management practices?**
    - Thankfully, yes. A lot has changed. Password management tools have become mainstream as more and more individuals and businesses have adopted them. But not nearly enough, as the Pew research suggests.
    - **On a personal level,** cyber-aware people have started using secure digital password managers across their devices. They have adopted 2-factor authentication, and have become more cognizant of the benefits of VPNs to further protect their passwords and other information. These individuals are aware of the value of password security and are more likely to practice better cyber hygiene in the workplace too.
    - **On a business level,** conscientious companies have installed enterprise-level privileged access management (PAM) software and are enforcing password management best practices across their organizations. PAM software has enabled companies to introduce automation to password management, so passwords can be changed, rotated, and expired on an automated schedule. Plus, passwords can be better managed when an employee leaves the company or when another high-risk event has occurred.
    - Password use can be tracked and reported on, and employees' actions can be monitored and recorded as they access the sensitive information protected by company passwords. And PAM software can help companies establish and prove compliance to fulfill their industry's audit requirements for protecting passwords.
    - Passwords are the staple of secure access to accounts and sensitive information. They will remain so for the foreseeable future, despite advancements in bio-metric authentication which simply augments passwords interactions.
    - Knowing that so many people and organizations are still not paying much attention to their cyber security practices, criminal hackers are reaping the rewards of this neglectful behavior and have been known to observe their victims for months before making any malicious moves.
    - With these things in mind, I have both high hopes and some predictions for password management in 2019
    - As we begin another year of online working, storing data, banking and more, I don't need a crystal ball to predict that 2019 will come with a generous helping of cyber-attacks and a side of ransom ware and phishing scams.
    - But I know for sure that we're armed with better security solutions and more knowledge than ever before, and I encourage you to embrace both immediately so that I can wish you a Cyber-Safe New Year with the knowledge that you have to tools to do it!

ISSN 2348 – 8034
Impact Factor- 5.070

- Chances are, what you use today would be referred to as a "static password." A static password is simply that: a password that, once set, is left unchanged. Hacking static passwords is not a difficult task for even your typical attacker – commonly used methods such as dictionary or brute force attacks is often enough to get the job done. If your password is left unchanged, it really is only a matter of time before it can be cracked (though there has been some new research on password expiration that puts that question directly into the limelight). While this bit of info is disconcerting, you can take measures on your own to protect the information and other data that is important to you. A good step in the right direction would be to use a dynamic password
- In fact, you may already be a user of dynamics passwords. One Time Passwords (OTPs) are a commonly used type of dynamic password – a machine generated, random string that is used once to authenticate. Every time an end user wants to login, instead of entering their usual static password every time, they would simply input a unique, machine generated password. This dynamic password can be received on a mobile phone or made by a dedicated security token. Dynamic passwords are convenient because they don't have to be remembered, and because the password is never the same, they serve as a major roadblock for hackers who may be looking to break into user accounts.
- It is time for the naysayers and the lovers of static passwords to begin to face the facts – the static password will become extinct. Whether it is an easy and quiet slip into the history books or whether we have to drag it kicking and screaming out the door, the static password is going to go away. The FIDO alliance (whose members include tech heavyweights such as Microsoft, Google, and others) has published a report for a system to eliminate the static password for good. I'll admit it, I do see a bit of an appeal for a static password – set a password once, and forget about it – but, we are at an age where too much is protected behind a simple string of never changing characters. We should begin to embrace the dynamic password, and with it, say farewell to password resets, changes, and hacker attacks.

10. CONCLUSION

Brute force attack is attempting to crack passwords as many times as possible. So in this lists of common passwords are also typically tested . Password strength is this password that cannot be guessed. Passwords which can be easily guessed is called weak passwords .Finally ,we can conclude that:

1.Don't use your login or username in any form.

2. Don't use your name personal information in passwords.

3. Do use a password with lower& upper case letter.

4. Do use a password that you can type &member

Therefore, by giving a string password we can secure the data stored in a file

Password is one of the sensitive information . So in this paper we have discussed how to maintain a password and also how to store details in file .So instead of memorizing all the passwords and IDs it is the best way to store them in a single file. Until you will not share the password of the file to other person it is safe and secure

11. WHY WE HAVE CHOOSEN

Particularly we have chosen this project because we have a habit of forgetting things .So, it is hard to remember all the passwords for multiple accounts. We thought of storing all the passwords in a single file and lock the file to secure the details

12. REFERENCES

[1].Adams,A.,&Sasse,& sasses,M.A(1999). Users are not the enemy. Association for computing machinery. Communications of the ACM.

[2] Anderson,, J.R.(1994). Learning and memory. An integrated approach: john willey & sons

[3] B. Dawnmedlin, & Cazier, J.A(2005). An investigative study: consumers password choices on journal of information privacy & security

[4] Burnett, m.(2002,march 7, 2002) ten windows password myths retrieved april 12, 2005,

[5] Hewett, K.L.(2001). Congnitive factors in design: basic phenomena in human memory and problem solving. Paper presented at the proceeding of the third conference on creativinty & cognition, loughborough,UK.

[6] Higbee, K.L.(2001). Your memory: how it works & how to improve it(2 ed.). new York, ny: Marlowe & company.

[7] lves, B., Walsh,K.R., & Schneider, H.(2004). The domino effect of password reuse. Association for computing machinery. Communications of the ACM.

[8] Miller, G.A (1956). The magical number seven, plus or minus two: some limits on our capacity for processing information. Psychological review, 64,81-97.

[9] Newell, A.,& Simon, H.A.(1972). Human problem solving. Englewood cliffs, NJ:prienticehall.

[10]sans.org.(2013). Password policy:www.sans.org.