Challenges in Password Memorization for Multiple Accounts of Single User

Pratik Ranjan[1], Nachiketa Tarasia[2]

[1]Research Scholar, School of Computer Engineering,
KIIT University, Bhubaneswar, India

[2]Assistant Professor, School of Computer Engineering,
KIIT University, Bhubaneswar, India

Abstract: ***Passwords are the most common way to authenticate the users and allow access to the system or any application. User Id and password plays vital role in any authentication based application. Numbers of online accounts are increasing with increase in services over internet that results increase in passwords as well. Ultimately it is upon users who need to remember their all passwords to access the online accounts. This paper is to deal with the problem related to remembering of passwords for any human being and how to overcome in near future.***

Keywords: *Authentication, Password, Security, User Id.*

1. Introduction

Technology helps human being to live in more comfortable way. It is the new developed technologies which makes our life safer while providing us the facility to access the system from anywhere in the world. These new technologies need to be simple enough so that it can be popular and easily adoptable by the human being.

Computer Security is a growing area of research. The basic security requirements for any computer system are (i) Confidentiality, (ii) Integrity, (iii) Authentication and (iv) Availability. Authentication deals with the very common way to access any system by using user-id (UID) with password. The pair data (user id and password) is use to verify authenticated user.

The user id and its corresponding passwords are increasing continuously. In any online service, new user can create an account and further access it using UID and password. This new account adds one pair of UID (some time calls login id or registration id) and password so that access can be possible next time. It is a growing list as internet is growing day by day and we are using the online services for every small need of our daily life.

Email accounts are the very common for most of the internet users and in many cases people have multiple email accounts. Computer systems have their own id and password. Different online services like online ticket booking system, online telephone bill payment system, online bank accounts, social networking accounts and many more are the examples where all need some identification with the passwords. These all services are growing by nature and hence create a big challenge for a human being to remember all. This paper deals with challenges in near future that what will be the scenario of these passwords and how a good research required that technically deal with it. The new technique must be simple enough so that it can't give extra burden to the user and user can enjoy the online services.

2. Current Process to Login Any System

The general method of authentication is to use UID with corresponding password. If both matches then allow user to access the system otherwise disallow the user and give some more chances to access the system. If user is unable to remember the passwords then provide the facility to recover the password or to reset the password.

The recovery of password can be done by answering some hint answers that was save with the system while creating a new account. This is also a kind of password that user should remember for password recovery. But if user is unable to answer correctly then the recovery of password has been done by some third party help like other email account linked with the existing one or the SMS service to generate OTP (One Time Password).

These all services are again linked with some UID and password of any other account or to the mobile number. But in worst case where one can't access the linked email or his mobile number is not in service then it is probably impossible to access it instantly. Then this problem may be solved by the administrator but it takes time.

So, what we observe here is that ultimately the user has to remember the passwords with the corresponding UID. The remembering power of any data varies from person to person. That makes sense that technology must do something new to deal with such a challenging field in the area of security.

3.1. Problem with existing process of Authentication

3.2. Initial Password setting criteria

It is very good to keep password to be secure enough so that it can provide security to the user. But the problem is that the remembering of that password is also important to access account next time. A password setting is depends upon

application and varies accordingly.

The common properties to set new passwords are: (1) Password must be alphanumeric with some special characters; (2) It should be of minimum length say 7 to 8 character, (3) It should not be simply any common name that user familiar with (4) UID and password must be different, (5) The password should be complex enough so that it can't be guessed or tracked easily i.e. it contain some combination of characters, digits and some special characters, (6) It should be updated on regular interval of time. (7) Users must not write it down their passwords neither in any physical paper, diary nor in any file in their desktop (8) It should not be saved in draft or in inbox of their frequently accessed accounts (9) Passwords of two different accounts must be different although the UID may same for both (10) It should not be share with any other person using any medium in any condition.

As we raised the problem with different points, it is very difficult for user to remember such a huge set of passwords. There are some instructions that must be followed by every user due to maintain secrecy. The passwords are so difficult to remember if user having 10-20 UID. And form the above points (5), (6) and (9) passwords are more difficult to remember for an old age person or person having weak memory. Though the remembering power varies from person to person but considering the above 10 points and due to increase in online accounts, for any single user it is really a tough job to remember the passwords.

3.3. Frequency of accessing accounts

The users who uses the services online or by using some authentication system can be categorized as (1) Very Frequently login user accounts (login an accounts 5-10 times daily) (2) Frequently login user accounts (login daily) (3) weekly login user accounts (like to access book movie ticket weekly) (4) monthly login user accounts (like monthly online bill payment) (5) rarely login user accounts.

A user can have different login accounts. If a user have all the five variety of accounts then s/he may be able to remember her/his very frequently and frequently login account's passwords but difficult to remember other passwords because they are not used on regular basis.

3.4. Types of Accounts

Users have different kinds of online accounts for their verity of uses. The common online accounts are (1) Email accounts (generally 2 accounts per user like Gmail id, Yahoo id etc) (2) Official mail account (3) Social networking accounts (Facebook, Twitter, Linkedin etc.) (4) Bank account UID.

Apart from these the user also need to remember the Pin Numbers associated with their Credit cards, Debit cards, Official secrete pin numbers to access their accounts.

4. Previous Work

Some of the previous works [2], [4], [8] present the new approach towards the authentication process. The major portion of these research supports to use Biometric techniques. Graphical approach is also a good alternative but still not so popular in most of the application.

5. Conclusion

The research shows that the new technology needs to be secure and usable so that user can use it without any hesitation. The password memorization is a drawback in current online login system. It will be a very serious problem in near future when more number of users doing their most of the work online.

6. Future Scope

By keeping the thing simple it is very important to do research and come with a completely new technique that will secure as well as simple so that every user can use online services easily and there will be no memorization criteria for huge set of passwords for every online account.

References

[1] M. Zviran, W. J. Haga, "Password Security: An Empirical Study," Journal of Management Information Systems, Vol. 15, No. 4, pp 161-185, 1999.
[2] A. Perrig and D. Song, "Hash Visualization: a New Technique to Improve Real-World Security," International Workshop on Cryptographic Techniques and E-Commerce, pp 131--138, 1999.
[3] J. Yan, A. Blackwell, R. Anderson, Alasdair Grant, "The memorability and security of passwords - some empirical results," Technical Report, University of Cambridge, 2000.
[4] H. Luo, P. Henry, "A Common Password Method for Protection of Multiple Accounts," The 14" IEEE 2003 International Symposium on Persona1,lndoor and Mobile Radio Communication Proceedings, 2003.
[5] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," In Proceedings of the IEEE, Vol. 91, No. 12, pp. 2019-2040, 2003.
[6] B. Lu, M. B. Twidale, "Managing Multiple Passwords and Multiple Logins: MiFA Minimal-Feedback Hints for Remote Authentication," In Proceedings of Interact 2003, Zurich. IOS Press 821-824.
[7] D. S. Carstens, P. R. McCauley-Bell, L. C. Malone, R. F. DeMara "Evaluation of the Human Impact of Password Authentication Practices on Information Security," Informing Science Journal, Volume 7, 2004.
[8] A.K. Jain, A. Boss, "Multibiometric Systems," Communications of the ACM, Vol. 47, No. 1, 2004.
[9] A. Conklin, G. Dietrich, D. Walz, "Password-Based Authentication: A System Perspective," In Proceedings of the 37th Hawaii International Conference on System Sciences, IEEE, 2004.
[10] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in

People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.

[11] D. Gafurov , K. Helkala , T. Søndrol, "Biometric Gait Authentication Using Accelerometer Sensor," Journal of Computers, Vol. 1, No. 7, 2006.

[12] B. Grawemeyer, H. Johnson "Using and managing multiple passwords: A week to a view," Interacting with Computers, 23 (3), pp. 256-267, 2011.

Authors Profile

Pratik Ranjan is a Research Scholar and a student of M. Tech. in Computer Science & Information Security, School of Computer Engineering, KIIT University Bhubaneswar. His area of interest is Computer Security and Secure Key Generation.

Nachiketa Tarasia is Assistant Professor in School of Computer Engineering, KIIT University Bhubaneswar. His area of research is Wireless Sensor Network, Network Security, Neural Networks and Expert System.