A Secured Login System Using Advanced Technique for Social Networks

Mr. S.Dinesh[1], Mrs. C.Chitra Devi[2]
[1]Student (MSc. Information Technology) & Rathinam College of Arts and Science.
[2]Assistant Professor Department of Information Technology & Rathinam College of Arts and Science.

ABSTRACT - The project is entitled “A Secured Login System Using Advanced Technique for Social Networks” is developed using ASP.Net as front end SQL Server as back end. The main objective of this project is to prevent users’ passwords from being stolen by antagonist in social networks. In this project we secure the user’s credentials in Five Different Techniques such as Random Password Login, Logout Number Login, Secret Little Function Login, Virtual Password, and Graphical Password. Initially, user must be registered in this website with their personal details and other necessary details. Then normal login process, it shows the usual way of logging with their registered Username and Password

1.INTRODUCTION

In this project “A Secured Login System Using Advanced Technique for Social Networks” we discuss how to prevent users’ passwords from being stolen by adversaries in online environments. We suggest password mechanisms in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security, where a virtual password requires a small amount of human computing to secure users’ passwords. A function/program is used to implement the password concept with a security for complexity requiring a small amount of human computing. We further propose several functions to serve as system recommended functions and provide a security analysis. For user-specified functions, we adopt secret little functions in which security is enhanced by hiding secret functions/algorithms.

In recent days, Internet has entered into our daily lives as more and more services have been moved online. Besides reading the news, searching for information, and other risk free activities online, we have also become accustomed to other risk-related work, such as paying using credit cards, checking/composing emails, online banking, and so on. While we enjoy its convenience, we are putting ourselves at risk. Most current commercial websites will ask their users to input their user identifications (IDs) and corresponding passwords for authentication. Once a user’s ID and the corresponding password are stolen by an adversary, the adversary can do anything with the victim’s account, which can lead to a disaster for the victim. As a consequence of increasing concerns over such risks, protecting users’ passwords on the web has become increasingly critical

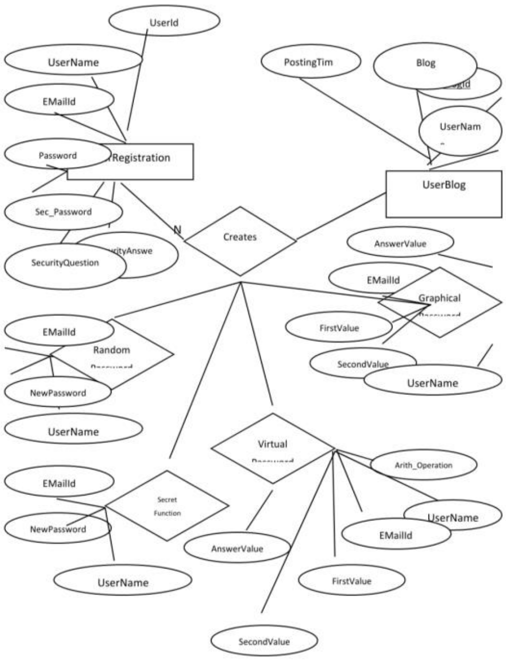


Fig:ERdiagram

A password is something that fits in the memory of a user, and the user chooses it. Since authentication is about verifying the user physical identity remotely (from the point of view of the verifier), the user behavior is necessarily involved in the process however, passwords rely on the part of the user which is most notoriously mediocre at handling security, namely his brain. Users simply do not grasp what password entropy is about. On the other hand, security of a physical token is much more "tangible" and average users can become quite good at it. "Password strength" can be somewhat improved by mandatory rules (at least eight characters, at least two digits, at least one uppercase and one lowercase letter...) but those rules are seen as a burden by the users, and sometimes as an insufferable constraint on their innate freedom. So the users become to fight the rules, with great creativity, beginning with the traditional writing down of password on a stick-up note. More often than not, password strengthening rules backfire that way.

1. Random password generation
2. Alternate Password Generation method
3. Secret little function Password- Position based Authentication
4. Graphical password generator
5. Virtual Password Generator

1. **Random password generation**

Random Password Generator is designed to help you create secure random passwords that are extremely difficult to crack or guess, with a combination of random lower and upper case letters, numbers and punctuation symbols. Random Password Generator is designed to create a much securer environment for either important data storage or privacy protection. It is able to generate highly secure random passwords that are almost impossible to crack. This smart and secure password generator also includes a useful Password Manager, by which you can mark, search, and organize the passwords generated.

2. **Alternate Password Generation method**

A traditional, static password is usually only changed when necessary: either when it has expired or when the user has forgotten it and needs to reset it. Because passwords are cached on computer hard drives and stored on servers, they are susceptible to cracking. This is especially a concern for laptops since they can be easily stolen.Unlike a static password, a Alternative password changes each time the user logs in with failed mandatory login. The passwords themselves are generated in one of two ways: either as time-synchronized or counter-synchronized using iterative and recursive methods. A recursive password generator can be written that is independent of the total number of password possibilities.

3. **Secret little function Password- Position based Authentication**

Secret little function is also known as Hash-based OTPs use cryptographic hashing algorithms to compute the password. As you know, a cryptographic hash is a one-way function that maps an arbitrary length message to a fixed-length digest. Thus, a hash-based OTP starts with the inputs (synchronization parameter, secret key, PIN), runs them through the one-way function, and produces the fixed-length password. Given an array of allowable password characters, e.g., chars, loop through each character (ch) in the array, recursively placing the character in each position (pos), until you have built up a character sequence (pwd) of the maximum size. The result will be all passwords of a given size. For example, suppose the recursive procedure is named GenerateAllPasswordsand you wanted all passwords of size eight. You would call the recursive procedure as follows: GenerateAllPasswords (“”, 0, 8).

4. **Graphical password generator** :

Graphical authentication scheme which is based on the Hash Visualization technique was been developed with reference to images. In that system, the user was asked to select a certain number of images from a set of program generated images. Later, the user was prompted to identify the pre-selected images in order to get authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS.

5. **Virtual Password Generator :**

Virtual password that requires secure users passwords in on-line environments to enabling the novel authenticated passwords. Regardless of the approach chosen, a user’s registration in the system is similar, i.e., the user submits a user ID and password. The one difference from a traditional approach is that in the virtual password scheme, there is a virtual function, which is a must, to be set during the registration phase. The server then delivers this function information to the user via some channels, such as, displaying it on the screen or email. The user needs to remember this function together with the password they have chosen or save them in disks or emails. The user-specified password and the system-generated function are combined into a virtual password. To authenticate a user, a system (S) needs to verify a user (U) via the user’s password (P) which the user provides. It is very reasonable that a password should be constant for the purpose of easily remembering it. However, the price of easy to remember is that the password can be stolen by others and then used to access the victim’s account. At the same time, we cannot put P in a randomly variant form, which will make it impossible for a user to remember the password. To confront such a challenge, we propose a scheme using a new concept of virtual password. A virtual password is a password which cannot be applied directly but instead generates a dynamic password which is submitted to the server for authentication.

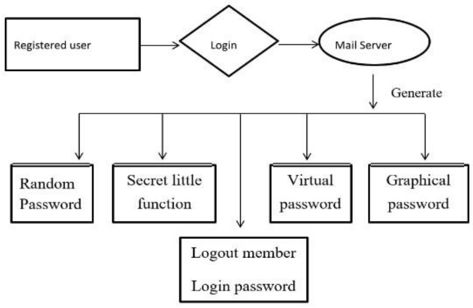


Fig: flow diagram

2.EXISTING SYSTEM

A password is something that fits in the memory of a user, and the user chooses it. Since authentication is about verifying the user physical identity remotely (from the point of view of the verifier), the user behavior is necessarily involved in the process however, passwords rely on the part of the user which is most notoriously mediocre at handling security, namely his brain. Users simply do not grasp what password entropy is about. On the other hand, security of a physical token is much more "tangible" and average users can become quite good at it. "Password strength" can be somewhat improved by mandatory rules (at least eight characters, at least two digits, at least one uppercase and one lowercase letter...) but those rules are seen as a burden by the users, and sometimes as an insufferable constraint on their innate freedom. So the users become to fight the rules, with great creativity, beginning with the traditional writing down of password on a stick-up note. More often than not, password strengthening rules backfire that way.

3.PROPOSED SYSTEM

Online Social Networks (OSNs) have become ubiquitous and changed the way that users interact online. There has been an enormous growth in the usage of OSNs in the past few years as users utilize OSNs to share a variety of information. This vast amount of information is valuable, and therefore introduces several privacy risks and challenges. In our work, we analyze the security and privacy issues in OSNs and present several techniques to enhance OSN security and privacy. These protective login methods are consistent on OSNs namely, Random password generation, Alternate Password Generation, Secret little function Password generation, Graphical password generation, Virtual Password generation. Our approaches highly benefit from using a secure and privacy aware social network.

3.1 ADVANTAGES OF PROPOSED SYSTEM

- Improved fraud detection and reduced fraud losses for issuer, this makes hacking useless.
- Security is improved by shifting the burden of data protection to large-scale operators like Facebook, Google, and PayPal.
- The cost of customer support required to help users who can’t sign in is similarly transferred.
- It’s less likely that your users will forget the more-commonly-used username/password combinations registered at their favorite social networking sites.
- No username/passwords are transmitted during the third-party authentication process, only authorization tokens.

System Implementation is the stage in the project where the theoretical design is turned into a working system. The most critical stage is achieving a successful system and in giving confidence on the new system for the user that it will work efficiently and effectively. The existing system was long time process. Implementation of this project refers to the installation of the package in its real environment to the full satisfaction of the users and operations of the system. This stage consists of

- Testing the developed program with sample data.
- Detection and correction of errors.
- Testing whether the system meets user requirements.
- Creating filters of the system with actual data.
- Making necessary changes as desired by the user.
- Training user personnel.

The implementation phase is less creative than system design. A system design may be dropped at any time prior to implementation, although it becomes more difficult when it goes to the design phase. The final report of the implementation phase includes procedural flowcharts, record layouts, and a workable plan for implementing the candidate system design into an operational designTesting is done individually at the time of development using the data and verification is done the way specified in the program specification. In short, implementation constitutes all activities that are required to put an already tested and completed package into operation. The success of any information system lies in its successful implementation.

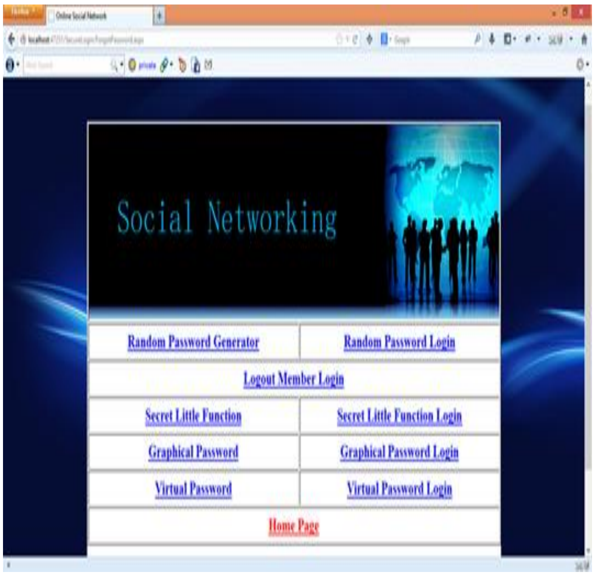
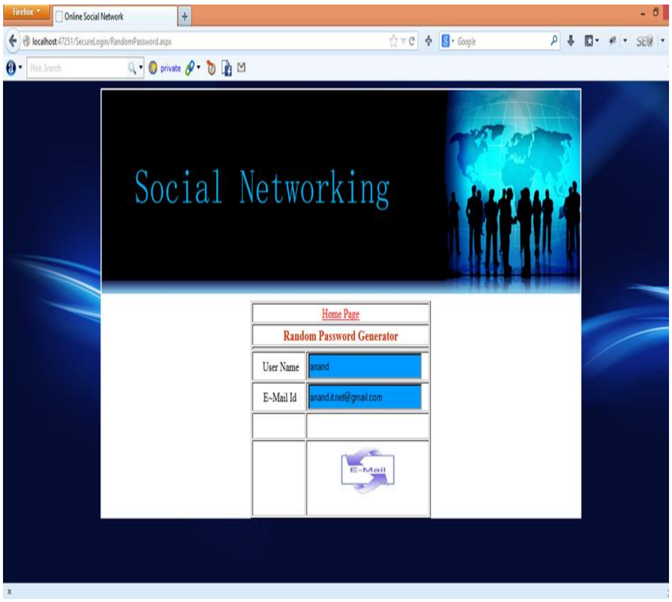


Fig: home page



User Name: anand

E-Mail Id: anand.it.net@gmail.com

Fig: login page

6.CONCLUSIONS

This project is developed and secured for the Online Social Networks. Advanced login techniques and Different types of technical controls, which form part of the body of a secured OSN, were evaluated with special emphasis on the incorporated new techniques such as Random Password Login, Logout Number Login, Secret Little Function Login, Virtual Password, and Graphical Password. User Access permissions for Social Network is developed and able to verify the identity of the user who is attempting to alternate access ways with secrete information exchanged with mail server

REFERENCES

[1] D. Sarunyagate, Ed., Lasers. New York: McGrawHill, 1996.

[2] O. B. R. Strimpel, "Computer graphics," in McGrawHill Encyclopedia of Science and Technology, 8th
ed., Vol. 4. New York: McGraw-Hill, 1997, pp. 279-283.

[3] T.K.Sethuramalingam, 2B.Nagaraj, “A Comparative Approach On Pid Controller Tuning Using Soft Computingtechniques”, International Journal of Innovations in Scientific and Engineering Research (IJISER), Vol.1, No.12, pp.460-465, 20114.

[4] K. Schwalbe, Information Technology Project Management, 3rd ed. Boston: Course Technology, 2004

[5] E. P. Wigner, "Theory of traveling wave optical laser," Physical Review, vol.134, pp. A635-A646, Dec. 1965.

[6] J. U. Duncombe, "Infrared navigation - Part I: An assessment of feasibility," IEEE Transactions on Electron Devices, vol. ED-11, pp. 34-39, Jan. 1959.

[7] M. Bell, et al., Universities Online: A survey of online education and services in Australia, Occasional Paper Series 02-A. Canberra: Department of Education, Science and Training, 2002.

[8] E.Rama Kalaivani,E.Ramesh Marivendhan,N.Suma,"Prediction of diabetes with hybrid prediction model using big data in health care",International Journal of Engineering and Technology,Vol 7,No 1.3. DOI: 10.14419/ijet.v7i1.3.8980