IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Secured Password Authentication using Image an Auto Dialing

Mr.S.Jambunathan[1], Gouthaman.P[2]

Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore[1]

M.Sc Computer Science, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore[2]

Abstract: This paper is developed as a web application which can be accessed universally. In this project user get their application form from the respective interested banking site. All that a normal user would have to do is to browse through the different pages of the site and do whatever transaction he/she wants. This proves to be much more beneficial and also more efficient to maintain than the conventional method of banking. These cards provide a safer way to use money from your personal account without using a check or carrying around large amounts of cash. Before this process the user has to register with their user name, password and image. During Registration user gives their personal details such as address, phone number, mail id. User will be intimated with banks rules and regulations. If the user wants to apply e banking means they can apply continuously. After this process bank will provide unique pin number to the registered user. Administrator will update the database with the information got from registered user. Now user gets the authentication to logon to the system, and also they can check their account status. User can also change their pin number and view their transaction. And also transfer their amount in locally or foreign exchange. To deposit or withdrawal amount from the banks manually is a time consuming process. To make this manual process fast this proposed system allows transferring amount another account. . This proposed system deals with all transactions of actual.

1. INTRODUCTION

The 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.

The secure protocol SSL/TLS for transmitting private data over the web is well-known in academic research, but most current commercial websites still rely on the relatively weak protection mechanism of user authentications via a plaintext password and user ID. Meanwhile, even though a password can be transferred via a secure channel, this authentication approach is still vulnerable to the following attacks: 1) *Phishing attacks*, phishes attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication; 2) *Password Stealing Trojan* programs contain or install malicious codes. Examples include: a) key loggers capturing keystrokes in the machine; and b) Trojan Redirectors redirecting end-users network traffic to a desired location; and 3) *Shoulder Surfing* steals others' sensitive personal information by looking over victims' shoulders or capturing users' inputs and screens by taking pictures and videos using cameras and video recorders, respectively. Many schemes, protocols, and software have been designed to prevent users from some specified attacks. However, to the best of our knowledge, there is not a scheme which can defend against all the attacks listed above at the same time.

In this paper, we present a password protection scheme that involves a small amount of human computing in an Internet-based environment or a ATM machine, which will be resistant to phishing scams, Trojan horses, and shoulder surfing attacks. We propose a virtual password concept involving a small amount of human computing to secure users' passwords in online environments.

The tradeoff is that stronger schemes are more complex. Among the schemes, we have a default method (i.e., traditional password scheme), a system recommended function, a user-specified function, a user-specified program, and so on. A function/program is used to implement the virtual password concept by trading security for complexity by requiring a small amount of human computing. We further propose several functions to serve as system recommended functions and provide a security analysis. We analyze how the proposed schemes defend against publishing, key logger, shoulder-surfing, and multiple attacks. In user-specified functions, we adopt secret little functions in which security is

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

enhanced by hiding secret functions/algorithms. To the best of our knowledge, our virtual password mechanism is the first one which is able to defend against all three attacks.

We further propose a scheme to adopt μTESLA to be used for re-keying and to defend against phishing. The proposed functions include secret little functions and two other schemes called codebook and reference switching functions. Our objective is to produce a function achieving both: 1) ease of computation; and 2) security. However, since simplicity and security conflict, it is difficult to achieve both. The idea of this paper is to add some complexity, through user computations performed by heart/hand or computation devices, to prevent the three kinds of attacks. There is a tradeoff of how complex the computation by the users can be. One goal is to find an easy to compute but secure scheme for computing. We believe that, for some sensitive accounts such as online bank accounts and online credit card accounts, users are likely to choose additional complexity which requires some degree of human computing in order to make the account more secure.

2. EXISTING WORK

In the Existing work the access code will be sent to the mobile using that user login to the website. Access code security is not there. We present a password protection scheme that involves a small amount of human computing in an Internet-based environment or an ATM machine, which will be resistant to phishing scams, Trojan horses, and shoulder surfing attacks.

2.1.1 DISADVANTAGES OF EXISTING WORK

- Attacks easily access our password
- In login time access code send to user mobile and then user login to account. Some time hacker hacking the database and seeing the access code and then use our account
- Hacker easily guesses the password
- Website designed by a simple format.
- Not using special software using in virtual password creation.

2.2 PROPOSED WORK

In the proposed work, a virtual password concept involving a small amount of human computing to secure users' Passwords in online environments. We proposed differentiated security mechanisms in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security. The function/program is used to implement the virtual password concept with a tradeoff between security and complexity and requires small amount of human computing. However, since simplicity and security conflict with each other, it is difficult to achieve both. We further proposed several functions serving as system recommended functions and provided a security analysis. We analyzed how the proposed schemes defend against phishing, key-logger, shoulder-surfing attacks, and multiple attacks. In user-specified functions, we adopted secret little functions in which security is enhanced by hiding secret functions/algorithms.

2.2.1 ADVANTAGES OF PROPOSED WORK

- It is provide high security
- Hacker maybe knowing our password but he cannot access our account because he did not create virtual password
- Special jar was designed to use creating a virtual password.
- Any types of hacking method cannot implement our account.

3. PROCESS

- **ADMIN:**

Admin is the only person having full access control and full permission in E-MONEY management system. He cans able monitor entire transaction in the E-MONEY. He performs following tasks.

- **APPLICATION:**

In this module admin monitor the user registrations and also check the Account, E-MONEY and net banking application form. And check he applied Net banking for which bank and user entered details are either correct or not.

- **IMAGE PIN PROVIDER:**

In this module admin acts like a manager. He see the Net banking applications and verify those details are correct or not. And provide the individual pin number for every application. This pointer is maintained secretly.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Because if any other else known this pointer means he can able to access our net banking and no secure for amount in net banking transaction. So it maintained secretly.

- **NET BANKING TRANSACTION LIST:**

In this module admin can view and monitor entire transactions that are performed using net banking. It helps to improve the bank access. In this admin monitor mobile recharge details, ticket reservation details, money transfer details and foreign exchange details.

- **USER:**

User is the person also having access control in E-MONEY but permissions to access. He performs following tasks.

- **USER REGISTRATION:**

Every user can register their details in this system to enter into this system, applying for E-MONEY and perform transactions. After registration user get user id and password to enter into this system.

- **APPLY FOR ACCOUNT:**

In this module user can apply for Opening an account in particular bank to maintain transactions. This module contains information about bank name, branch name, account number, user details, id proof and introducer details. Their user details are maintained very secretly no one can view the details. And user can simultaneously apply for E-MONEY and net banking.

- **APPLY FOR E-MONEY:**

In this module user can apply for E-MONEY. Using this module user can easily apply for E-MONEY. This module contains customer name. Address, contact details and account number.

- **APPLY FOR NET BANKING:**

In this module user can apply for Net banking. This module helps the user to easy money transfer through net banking. This module contains customer name. address, contact details and account number.

3.1 INPUT DESIGN

Input design is the process of converting the user-oriented. Input to a computer based format. The goal of the input design is to make the data entry easier, logical and free error. Errors in the input data are controlled by the input design. The quality of the input determines the quality of the system output.

The entire data entry screen is interactive in nature, so that the user can directly enter into data according to the prompted messages. The users are also can directly enter into data according to the prompted messages. The users are also provided with option of selecting an appropriate input from a list of values. This will reduce the number of error, which are otherwise likely to arise if they were to be entered by the user itself.

Input design is one of the most important phases of the system design. Input design is the process where the input received in the system are planned and designed, so as to get necessary information from the user, eliminating the information that is not required. The aim of the input design is to ensure the maximum possible levels of accuracy and also ensures that the input is accessible that understood by the user.

The input design is the part of overall system design, which requires very careful attention. If the data going into the system is incorrect then the processing and output will magnify the errors.

The objectives considered during input design are:

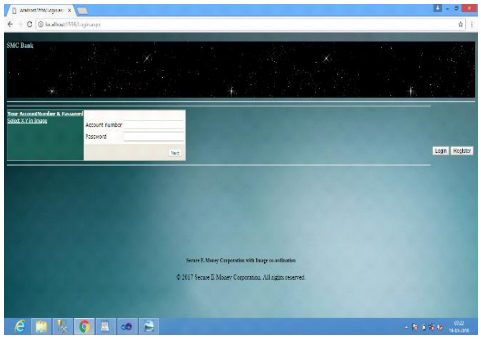
- Nature of input processing.
- Flexibility and thoroughness of validation rules.
- Handling of properties within the input documents.
- Screen design to ensure accuracy and efficiency of the input relationship with files.
- Careful design of the input also involves attention to error handling, controls, batching and validation procedures.

Input design features can ensure the reliability of the system and produce result from accurate data or they can result in the production of erroneous information.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018



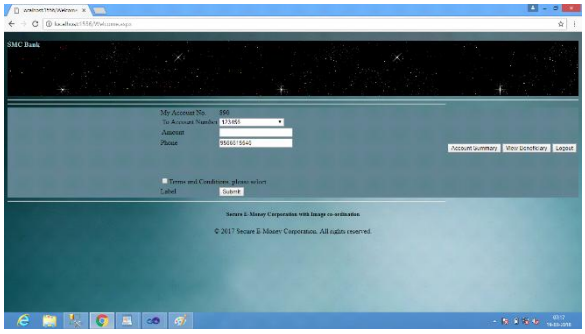
3.2 OUTPUT DESIGN

Output design is very important concept in the computerized system, without reliable output the user may feel the entire system is unnecessary and avoids using it. The proper output design is important in any system and facilitates effective decision-making. The output design of this system includes various reports.

Computer output is the most important and direct source of information the user. Efficient, intelligible output design should improve the system's relationships with the user and help in decision making. A major form of output is the hardcopy from the printer.

Output requirements are designed during system analysis. A good starting point for the output design is the data flow diagram. Human factors reduce issues for design involved addressing internal controls to ensure readability.

An application is successful only when it can provide efficient and effective reports. Reports are actually presentable form of the data. The report generation should be useful to the management for future reference. The reports are the main source of information for user's operators and management. Report generated are a permanent record of the transaction occurred. After any valid transactions; have commenced the report of the same are generations and: filed for future reference. Great care has been taken when designation the report as it plays an important role in decision-marking.



4. SYSTEM TESTING

It is the process of exercising software with the intent of finding and ultimately correcting errors. This fundamental philosophy does not change for web applications, because web based system and applications reside on network and inter-operate with many different operating systems, browsers, hardware platforms and communication protocols. Thus searching for errors is significant challenge for web applications.

4.1 TESTING AND METHODLOGIES

System testing is the state of implementation, which is aimed at ensuring that the system works accurately and efficiently as expect before live operation, commences. It certifies that the whole set of programs hang together System testing requires a test plan that consists of several key activities and steps for run program, string, system and user acceptance testing. The implementation of newly design package is important in adopting a successful new system

Testing is important stage in software development. System test is implementation should be a confirmation that all is correct and an opportunity to show the users that the system works as they expected it accounts the largest percentage of technical effort in software development process

4.2 UNIT TESTING

Here each program is tested individually so any error apply unit is debugged. The sample data are given for the unit testing. The unit test results are recorded for further references. During unit testing the functions of the program unit validation and the limitations are tested.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Unit testing is testing changes made in a existing or new program this test is carried out during the programming and each module is found to be working satisfactorily. For example in the registration form after entering all the fields we click the submit button. When submit button is clicked, all the data in form are validated. Only after validation entries will be added to the database.

CODING->DEBUGGING->UNIT TESTING->INTEGRATION TESTING

4.3 VALIDATION TESTING

Software validation is achieved through a serious of testes that demonstrate conformity with requirements. Thus the proposed system under consideration has been tested by validation & found to be working satisfactory.

4.4 INTEGRATED TESTING

Integrated testing is a systematic technique for constructing tests to uncover errors associated with interface. Objective is to take unit tested modules and build a program structure that has been dictated by design

4.5 ACCEPTANCE TESING

Acceptance testing involves planning an execution of a functional test, performance test and stress test to verify that the implemented system satisfies the requirement. The acceptance testing is the final stage of the user the various possibilities of the data are entered and the results are tested.

4.6 OUTPUT TESTING

Asking the user about the format required by them tests the output generated by the system under consideration .It can be done in two ways, One on screen and other on printer format. The output format on the screen is found to be correct as the format designed n system test.

5. IMPLEMENTATION PROCEDURES

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 a operational design.

5.1 USER MANUAL

The summary of important functions about the system & software can be provided as a document to the user. User training is designed to prepare the user for testing and convening a system. The summary of important functions about the system and the software can be provided as a document to the user.

6. SYSTEM MAINTENANCE

Maintenance is actually implementation of the review plan as important as it is programmers and analyst is to perform or identify with him or herself with the maintenance. There are psychologically personality, and professional reasons for this. Analyst and programmers spend fair more time maintaining programmer then they do writing them Maintenances account for 50-80% of total system development. Maintenance is expensive .One way to reduce the maintenance costs are through maintenance and software modification.

7. CONCLUSION

Password is the most commonly used method of authenticating users entering computer systems, passwords are frequently targeted by attackers wanting to break into systems. It is critical that this first line of defense against unauthorized access is effective by rigorously practicing good password management policies. Different passwords should be used for different systems with respect to the security requirements and the value of information assets the need to be protected. Make use of other access control mechanisms to facilitate password management and reduce the effort required by users in memorizing a large number of passwords. This should be enforced with good security policies and guidelines, supported by user awareness training and education on the best practices in choosing and handling passwords. In addition, for effective information security management, consideration should also be given in areas including but not limited to physical References.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

8. FUTURE ENHANCEMENTS

The scope of the paper can be further improved by using various techniques like picture password. The passwords can't be changed every minute, thus making the user free from remembering passwords. The "SECURED PASSWORD AUTHENTICATION USING IMAE AND AUTO DIALING" is just providing better security password to online mode. Every individual does not have to register on each and every website. Passwords are generated every time the user has to login. The system combines picture passwords along with a handheld device and sound signature to form a multifactor authentication system. The generation of random click points during the online mode prevents the shoulder surfing attack as well as dictionary attacks. Storing the images at the server provides better security as compared to offline mode.

REFERENCES

Text Books

- .Elias Awath, "SYSTEM ANALYSIS AND DESIGN", Tata Mc Graw Hill Publication, Sixth Edition,2003
- .S.Ramachandran,"COMPUTER AIDED DESIGN", Air Walk Publication, Third Edition,2003
- .Richard Fairley, "SOFTWARE ENGINEERING CONCEPTS", Tata Mc Graw Hill Publication, Second Edition,1997
- .Distributed .NET Programming in VB .NET by Tom Barnaby
- Professional VB.NET, 2nd Edition by Fred Barwell, et al
- The .NET Languages: A Quick Translation Guide by Brian Bischof

Websites

http://www.pocketlint.com/news/124283-password-managers-explained-the-best-apps-availableand-why-you-need-one
https://www.pentestpartners.com/blog/concerned-about-keefarce-dont-be-whyyou-should-still-use-a-password-vault/
http://www.tripwire.com/state-of-security/securityawareness/a-lastpass-hack-with-a-happy-ending/
http://www.martani.net/2014/07/thoughts-on-dashlane-password-sharing.html