RESEARCH SCRIPT IJRCS - International Journal of Research in Computer Science ISSN: 2349-3828

ERANDP METHOD OF SECURED PASSWORD PROTECTION

VEENAA DEEVE NV*, VIJESH JOE. C*, K. NARMATHA*
*Assistant Professor, Department of Information Technology,
Karpagam College of Engineering, Coimbatore
Veenu8190@gmail.com,vijesh.joe@gmail.com,knarmatha18.cool@gmail.com

Abstract—*Security plays a very important role especially for the internet users. The number of online transactions and secure information exchange is increasing day by day. The problem of security is solved with many solutions, but along with the increase in number of solutions, the way in which the attackers hack or phish the system is also equally increasing. In our work, we are mainly concentrating on the various attacks that can cause problem in the system and also the way in which it can be avoided. The hacking attacks are mainly concentrated where it is tried to be handled by using a different kind of ElGamal based Randomly Generated Dynamic Password Security (ERANDP) method. This method ensures the users to feel safe while using the internet as they are getting three level of security while passing the sensitive information in the online portal. The use of random functions is considered to be the best suggestions for improvising the security against phishers, key loggers and also the attackers of shoulder-surfing. Instead of using the same user-defined function, the choice of dynamic random function can help the user's information security to a great deal. The system model used for implementing this security in the system is considered to be highly efficient and useful for almost all the users.*

Keywords—ElGamal Encryption function, ERANDP, virtual password, password protection, OTP security.

I. INTRODUCTION

It is nowadays impossible for any individual to make their transactions and works completed without the help of internet. Almost all the fields has taken its stand in the market of internet. So the need and importance for implementing security in the system has raised to a greater extent. The main interest for the attackers not only lies in the traditional transaction based secure sites but also on the information storage data stores. The data store has vivid sort of information for providing the best and vital information for the users. Most of the users are not understanding the need for security level to be given for any data store in the first place. The types in which attack can happen is highly influencing the daily routine of the normal users. The general security parameters which will ensure security to the users are the user identification number and the password which is considered as the highest level of security in the current period of time. The security in the eyes of users stops when they don't reveal the security credentials to others.

The actual security attack need not be happened in the user side but also in the server level. If an attacker can hack the banking system data store or any other highly secure data store then there will be no need for them to get the individual password and user id from the user as they can directly get their hands on the secure information.

The need and importance of this three level security of using the RANDP method is increasing at this scenarios. Instead of relying on the security only provided to the users' security credentials, it will be helpful to have the randomly generated password with the dynamic functions.

The security protocols like SSL/TLS for transmitting data in a private mode on web is considered to be the main area for academic research for securing the system against various levels of attacks that can actually happen in a system. The protocols can works so well and are good are providing the security, until it come across the following kind of attackers as: 1. *Attackers* acquiring sensitive information by directly impersonating as a trustworthy person or business in any mode of electronic communication as phishers. 2. *Trojan programs* which contain malicious codes that can steal vital password related information through methods used by *key loggers* who will trace the key strokes of the users, *Trojan re directors* which will mainly concentrate on weighing the system with network traffic causing problem to the users while accessing the system. 3. *Shoulder surfing* method where the attackers will capture the user password credential based inputs directly by viewing the screens or pictures.

The number of schemes that are assigned for generating this secure password while secure transformation of the data is high. The ElGamal encryption technique is highly encryption technique which is playing a very important role in generating the secure OTP which cannot be guessed by any users in the first place. In method of ElGamal encryption itself the security level of key generation is two levels.

Related Methods:

The password generation method that is been used here is following the ElGamal [3] suggested algorithms resulting the virtual password to be generated. The use of system recommended function, a user-specified function or a user-specified program, etc can be used as one of the parameter for the function.

The concept of virtual password involves a minimal amount of human computing involved so that the security for the users' password can be secured. The most advantageous factor about this scheme is that there will freedom for the users to choose the preferred password generating function with various levels of security. [9] The security level can be finalized with the kind of function that

the individual is going to choose for the particular secure password generation.

A function/program is used to implement the virtual password concept by trading security for complexity by requiring a small amount of human computing. There are several functions to serve as system recommended functions and provide a security analysis. The proposed schemes defend against phishing, key logger, shoulder-surfing, and multiple attacks. In user-specified functions, secret little functions is adopted in which security is enhanced by hiding secret functions/algorithms.

The virtual password mechanism [1] is chosen over all other methods or techniques that is available because it is protecting the system against all three kinds of attacks like the phishing, key loggers and also the attackers of shoulder-surfing and multiple attacks. The hiding secret function/algorithm like the ElGamal encryption algorithm is providing the following advantages like 1) ease of computation 2) high security.

The problem with this method is the complexity in the scheme for computation. When the sensitivity of the accounts that are used is high in its significance level, the complexity of the functions that is been used is also increasing parallel.

II. AREA OF STUDY

Phishing

Phishing is a method used by security attackers in grabbing the vital information and credentials that are entered by the users directly in the impersonating or fake sites created by the attackers. The users will not have any idea that they are giving their important credential details directly to the fake site. The various ways in which the [5] phishing attacks can happen are phishing where the password credentials can be masqueraded impersonating as a trustworthy person; Spear Phishing done on certain individual for the sake of attack based on the personal information that is been gathered through many ways; clone phishing is a kind of phishing method where the individuals will be able to access and view all the emails that are cloned as they are identical.[10],[8] Here the users will not be aware of the impersonating as they both receive the original email; the attackers targeting senior executives and high profile persons are considered as whaling kind of phishing; MitM is man in the middle attacks where the attackers will be compromise all the data from the users by acting as a tool in sslstrip.

Browser Authentication for Strong Password Authentication

The problem of generating authenticated password with the browser extensions seems to be the better idea where there will be ways in which the individuals can actually defend themselves from password phishing. The PwdHash is a method which is used for attaining this sort of security. These extension in the browser will actually provide the individuals to obtain a cryptographic hash function dynamically in combination with the plain text.[5] Thus the use of password at one site cannot be used in another site. Some of the challenges which will affect the working of the whole system can be depicted. The most important among them is on secure client relationships with multiple servers where the clients will be having provision for creating and establishing a secure and also pseudonymous relationship with multiple servers. [1] The relationship can be either strong or weak on each interaction preserving the true identity of the user. The scalability and mobility while using this method is also high. The need for using this sort of alternatives for protection is considered to be vital for almost all the authentication methods that are preferred in recent days.

Shoulder-Surfing Resistant Graphical Password Scheme

The use of CHC (Convex Hull Click)[2] where the individuals has to prove himself to the system by clicking on different location to prove the identity like password images. Thus the vigilance will not be able to identify the password that is been directly given as password.[4] The public places authentication can only be achieved through the ways like this. There surveys which are proving the success in attaining the security of the system when the users were able to enter all the password images in a proper order without any discomfort in the first place.

III. WORK FLOW

The system is been divided into five main categories thus representing the working of the whole system in a much efficient manner to be understood by everyone as follows:

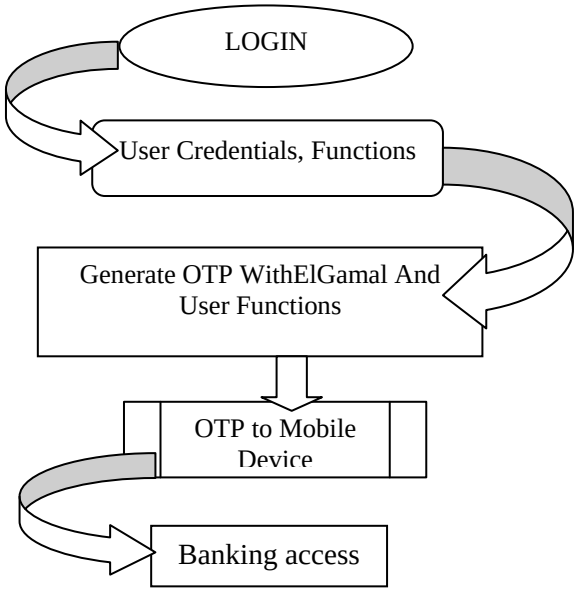

Fig. 1: Block Diagram of ERANDP system

1. Banking
2. Registration
3. Login

a. Elgamal Calculations
4. Account information
5. Financial Transactions

1. Banking

The individuals are nowadays used to purchase almost everything from the online sites, most of the official membership and other important tasks has become online and hence the online banking is playing a very vital role in the first place. Hence it is difficult for them to adapt just for the sake of security back to the paper mode which was used before. The system mainly intend on providing such sort of security which will ensure the individuals against all the odds related to the system and password security that is breached every now and then. The working is mainly on the basis of three main steps as the registration of the user where the user will be choosing the level of security needed, the second vital step for the working of the system is calculating the OTP based on the ERANDP method which is solely designed for the sake of securing the information, thirdly the use of the best virtual password method that could be sent to any mobile device used by the user directly acting as the authentication handler while accessing the system.

2. Registration module

The registration module plays a very important role in providing the security where the users who login in the system will be given access to download a jar file. The login form can be accessed and logged in only with the jar file that has been downloaded. The jar file is a form of expression calculation which varies user to user and is stored in a database for the best use of the users.

3. Login

The login page is something that will help the users in getting the name and password of the user based on the jar files. The user has to install the jar file in their local system for accessing such sort of private and secure information. The user has to enter the password for the system.

4. Online account transaction

It is the part of the whole system where the users will be accessing all the information in the system along with the transfer of the amount to other accounts which is highly sensitive when compared to all other information. The account holders would have entered all their personal information at the time of registration itself and the registration involves the users to choose the best way in which their own OTP can be generated. Hence there will be a virtual password that will be created by the users' suggested virtual function at the time of registration and also the ElGamalecryption technique in which the function generated key and the function will be given as an input and hence the best OTP will be generated. The generated OTP will be sent to the users mobile device which will be used for future reference and also to ensure security in the system.

5. Financial intelligence:

The financial intelligence is one such area where the individuals has to concentrate more and to filter the money transactions by providing the access to the system if and only if the system has three levels of security as the ERANDP method suggested.[3] The use of this sort of Suspicious activity report for checking the system before transferring amount to another account is highly recommended for ensuring the security in a much better manner.

Money Transaction Report:

This is the report generated based on all the transactions that are made on the account which does not involve in secure information in the first place. Hence the individuals can be carefree on the breach of security in their login.

IV.STIMULATION RESULT

The stimulation result on implementing the Erandp algorithm has been shown below in step by step process.

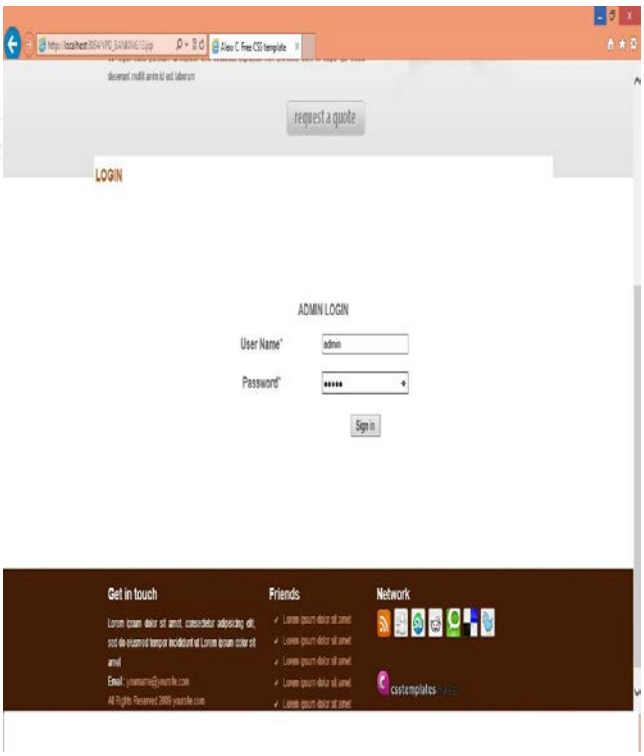

Fig 2: Admin Login

Fig. 2shows the representation of the login page where the user can become a new user by registration or by just logging in with the user id password that they have already given.

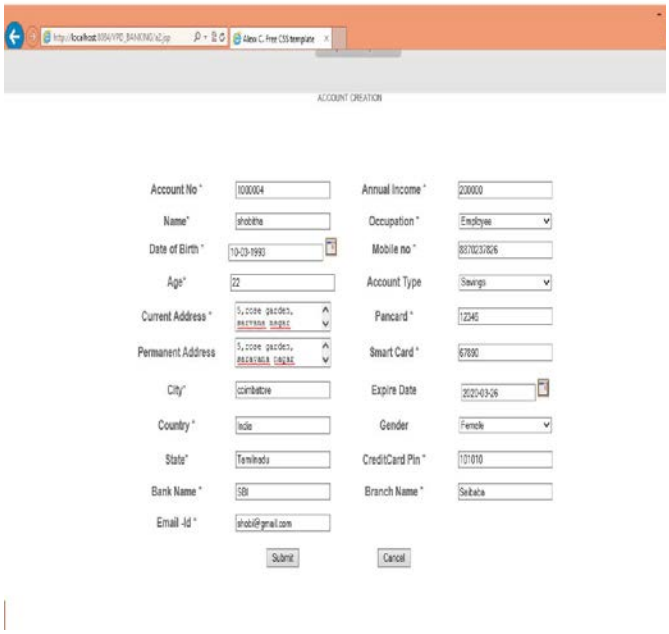

Fig 3: Account Creation

Fig. 3 is the representation of creation of the account in the banking system and getting support for making the other banking activities.

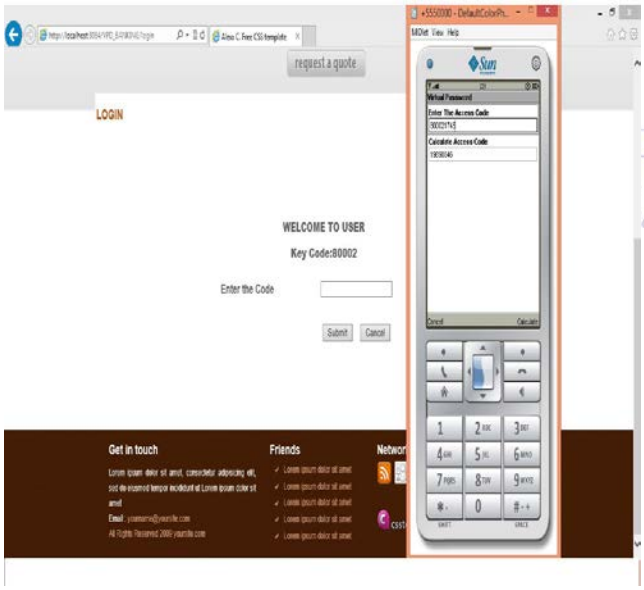

Fig 4: Key Code

Fig. 4, depicts how the jar file can be downloaded and the further steps explaining how the installation of this jar file lead to a generation of a passcode. The passcode which is generated while installing the jar file will be directly sent to the mobile emulator and hence it is been used for accessing all the important details. Thus the three levels of security can be ensured for safety transaction in the online banking, helping all the users to continue banking without any hesitation regarding the security of the system that they are using.

V. CONCLUSION

It is found that the system-generated functions are used in its best manner to get the input tokens including the keys with functions. The security level is increased as there is three level of checking including the steps of jar file installation, generation of the keys based on the unknown function based on the jar file and the input given to the ElGamal encryption algorithm in the first place. The users who are using this system in their own mobile device felt so satisfied with the system.

VI. REFERENCES

[1] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchel, “Stronger password authentication using browser extensions,” in Proc. 14th USENIX Security Symp.

[2] E. Gabber, P. Gibbons, D. Kristol, Y. Matias, and A. Mayer, “On secure and pseudonymous user-relationships with multiple servers,” ACM Trans. Inform. Syst. Security, vol. 2, no. 4, pp.
390–415, 1999.

[3] Benoit Chevallier-Mames, Pascal Paillier, David Pointcheval, “Encoding-Free ElGamal Encryption Without Random Oracles”, in Proc. 9th International Conference on Theory and Practise in Public Key Cryptography PKC 2006.

[5] Anti-Phishing Working Group. [Online]. Available: http://www.antiphishing.org

[6] J. R. Levine. (2004, Apr.). A Flexible Method to Validate SMTP Senders in DNS [Online].Available: http://www1.ietf.org/proceedings−new/04nov/IDs/draft-levine-fsv-01.txt

[7] V. A. Brennen. (2004). Cryptography Dictionary, vol. 2005, 1.0.0 ed.[Online]. Available: http://cryptnet.net/fdp/crypto/crypto-dict/en/cryptodict.html

[8] [Online]. Available: http://www.bell-labs.com/project/lpwa

[9] E. Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, A. Tironi,and L. Zaniboni, “Spam attacks: P2P to the rescue,” in Proc. 13th Int.World Wide Web Conf., 2004, pp. 358–359.

[10] E. Gaber, P. Gobbons, Y. Mattias, and A. Mayer, “How to make personalized web browsing simple, secure, and anonymous,” in Proc.Financial Crypto, LNCS 1318. 1997.