Enhancing Security of E-Commerce Transactions using Noisy Password Technique

Komal K. Kumbhare
Student
Department of Computer Engineering
B. D. College of Engineering
Sevagram - 442102, India

K. V. Warkar
Assistant Professor
Department of Computer Engineering
B. D. College of Engineering
Sevagram - 442102, India

ABSTRACT

There are different methods that are developed for authenticating the users. The most common authentication method is text-based passwords. In this method, users are asked to enter their user ID and password. But the traditional text-based passwords are vulnerable to the attacks like shoulder surfing or peeping attack, key loggers, Trojan attacks, phishing, etc. In this paper, an alternative to the static text-based passwords is used to enhance the security of e-commerce transaction. This scheme is called Noisy Passwords. Noisy password technique is resistant to the eves dropping or shoulder surfing. It consists of actual password and variable alphanumeric noise.

General Terms

Noisy password, OTP, Noise, Actual Password;

Keywords

Noisy password, e - Transaction, OTP

1. INTRODUCTION

E-Commerce is the trading of products with the help of communication technologies. Most of the transactions in business are performed using computer network. Hence security of e-commerce transaction is very essential.

There are basically three main areas in which authentication methods are divided i.e. Token based authentication, Bio-metric based authentication and knowledge based authentication. Among these authentication, the most widely used authentication schemes are text-based and picture-based password.

The text-based passwords are non-resistant to finger attacks, dictionary attack, shoulder surfing, key loggers, Trojan attack, phishing, etc. Many times users use their accounts in public areas like cafe, hotel etc. In such situations, there are chances that any third party or an intruder uses a CCTV footage or hidden camera to record keystrokes. By simply recording the keystrokes, an unauthenticated user can gain access to the account of victim. Again the static text-based passwords are nonresistant to the Key loggers. Key loggers is program that creates a file containing the sequence of the keystrokes and sends it back to the attacker or store the file on the machine itself. Such type of problems can be overcome by assigning random password to the user. But they are difficult to remember.

Most commercial website uses static text-based passwords for authenticating their user. Generally users use short length passwords which may be related to their date of birth, some name, mobile number or place. The passwords with large length are difficult to remember. Hence static text-based passwords can easily be accessed by the attacker by using different methods. Today attacker can intrude by simply shoulder peeping the user because of wide view angles of laptop screens. To overcome the problem of shoulder surfing or eves dropping, a new password technique was proposed by [6], called noisy password. The noisy password scheme is a combination of various parts i.e. the terminator set, the actual password and the noise. Every time whenever the users want to access their account, they have to enter different string of alphanumeric characters, actual password embedded in it.

This paper presents the implementation of a noisy password technique. This paper has been organized as follows. In section II, related works and literature survey is described. The proposed system is presented in section III. Section IV discuses the implemented noisy password scheme. At last section V gives the conclusion.

2. RELATED WORK

The One-Time Passwords provide high degree of security to the system. But the security of communication of OTP is also essential. The system given in [1] provides high degree of security. They have combined the ECC with the palm vein bio-metric. The drawback of this system is that, it limits the number of users since the implementation cost of the system is very high. Biometric technique is one of the authentication methods, which is highly secured. But the costs of bio-metric devices are very high.

Reusable passwords or static text-based passwords are prone to the different types of attacks. One Time Passwords adds extra security to the system but due to inconvenience and cost of generator, it has some limitations. One-Time Algorithms [12] protects accounts of users but the degree of security is very minimal. Tsuji and Shimizu developed a protocol, One-Time-Password Authentication protocol, which was resistant to the replay and theft attacks. But after sometime, Wen-Chung Kuo and Yung-Cheng Lee [9] proved that this protocol is non-resistant to the modification attack.

There are two commonly authentication methods, text based and image-based authentication. For local and remote authentication, the image based authentication is implemented by [10]. Though the image based passwords are more user friendly as compared to the text based passwords, they are vulnerable to the shoulder surfing attack. Different types of attacks are discussed in [10].

To eliminate the drawbacks of simple text-based passwords, the solutions are proposed by [3]. Authors have developed the authentication system by using images. But the system is vulnerable to the password attacks. Methods, picture recognition, object recognition and pseudo-word recognition are sketched in [11].

A system proposed in [5] has high degree of security. They combined the OTP, SMS Gateway and MD5 hash function. Authors have minimized the delay time to 3 min that hackers will not get time to attack or eavesdrop. To overcome the drawbacks of one-time-password and traditional static text-based passwords, the new password scheme is proposed by [6], called noisy password. Noisy password proposed by [6], consists of four parameters, actual password or fixed set, terminator, safeguard number and the variable set i.e. noise. All the parameters are of alphanumeric variable length. The noisy password is resistant to the shoulder surfing attack. But the system was not user friendly. The error rates of the system were high. To reduce the error rate they proposed same scheme include time delay. It seems that the percentage error in password entry of noisy password but less than PEN technique as shown in [7].

3. PROPOSED SYSTEM

The proposed system has the combination of three different security techniques. The very first authentication technique is Noisy Password. The Noisy password is a combination of three different parameters, actual password, fixed set and terminator set. The second authentication technique is biometric based. In the proposed system, voiceprint is used, which provides high degree of security. And to ensure the security of e-commerce transaction, OTP mechanism is used.

Figure given below describes the architecture of the proposed system. The architecture has three modules as follow.

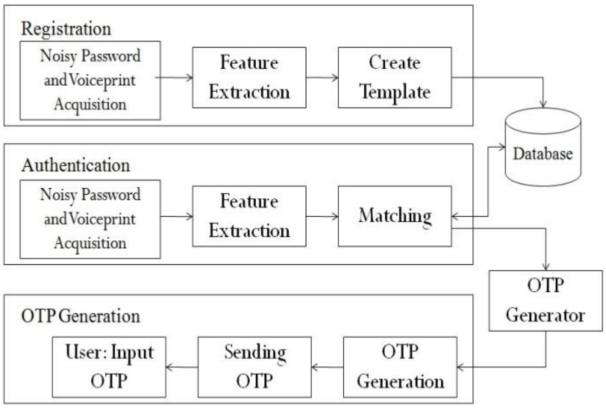

Fig 1: The Proposed System

3.1 Registration

Bio-metric techniques requires enrollment of users first and then further task like authentication using verification and identification is done. First of all users voice-print are acquired through recording device and then same are filtered for registration purpose along with their personal details. The pre-processing will be done on voice sample of user and the created template will get store in database. This voice template will be used by Speaker Recognition System. Noisy password is a combination of fixed set, terminator set and variable set i.e. noise. It contains actual password embedded with noise. The user have to provide a fixed alphanumeric and terminator set of noisy password at the time of registration.

3.2 Authentication

After successful registration, user will be able to login in E-commerce web application. User can access to their account by using his user ID and variable length Noisy Password. To perform e-transaction, he has to upload his real time voice sample. Speaker Recognition system will pre-process the voice sample to create voice template. This voice template will be matched with the existing template for that particular user ID in database. In this way the user will be identified and verified.

3.3 OTP Generation

Today most of the e-commerce transactions are done by using OTP mechanism. But using OTP generator or applying hash function is not enough. In proposed system, the OTP message will be encrypted by using Elliptic Curve Cryptography. ECC uses public and private key for encryption and decryption. It creates private key by applying hash function to the voice template that is created at the time of authentication as well as public key. This public key will be used by OTP generation to encrypt OTP message. At the client side, OTP will be decrypted by using private key of the user and then user may use this OTP to perform e-transaction.

4. NOISY PASSWORD

In this paper, the noisy password is used as an alternative to traditional static text based passwords. Noisy password consist of actual password (F), Terminator set (X) and the Variable set (V). All the three sets are of variable alphanumeric type. The following section describes the algorithms for selecting the noisy password and extracting the actual password from the noisy password at the time of authentication.

4.1 Selecting Noisy Password

In conventional authentication system, userID and the corresponding password are used for the authentication. In the proposed system the traditional password is replaced by the noisy password. Same as the traditional password, user have to register themselves by providing the part of noisy password, i.e. actual password (F) and terminator set (X) in such a way that the length of both, actual password and terminator set must be same. Fig 2 shows the flowchart for selecting the noisy password. At the time registration, user will be asked to enter their userID, actual password and terminator set along with their personal information. This information will get store in database.

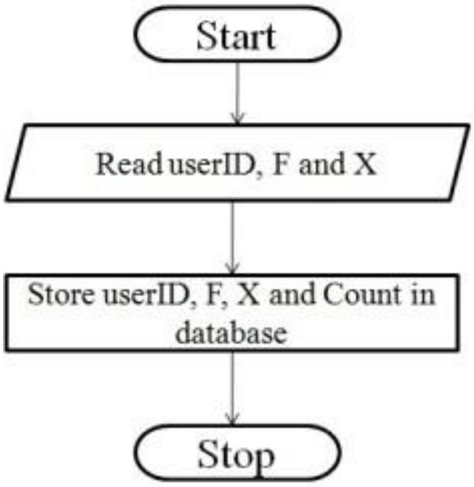

Fig 2: Selecting Noisy Password

Algorithm 1 Selecting Noisy Password

1. Read userID, actual password (F), Terminator Set (X) from the user in such a way that the length of actual password and terminator set is equal.
2. Store the actual password and Terminator in the database for the userID and initialize the counter variable count.

4.2 Authenticating User

Just like normal client server architecture, server will ask the user to enter their user identification (userID) and the corresponding password (pwd). Here the difference is that, user have to add noise in the actual password. There is no need to remember the noise part. It can be different for every time user accesses his account. He has to remember only the actual password and the terminator set.

The extraction of the actual password is the sole responsibility of the server. The subset of terminator set denotes the end of subset of noise or variable set (V) and the beginning of the subset of actual password. Since every time the user access his account using different password, it makes the system resistant to the shoulder surfing or peeing attack and key loggers, etc. Now if user wants to change his password, he may change either actual password (F) or terminator set (X) or both.

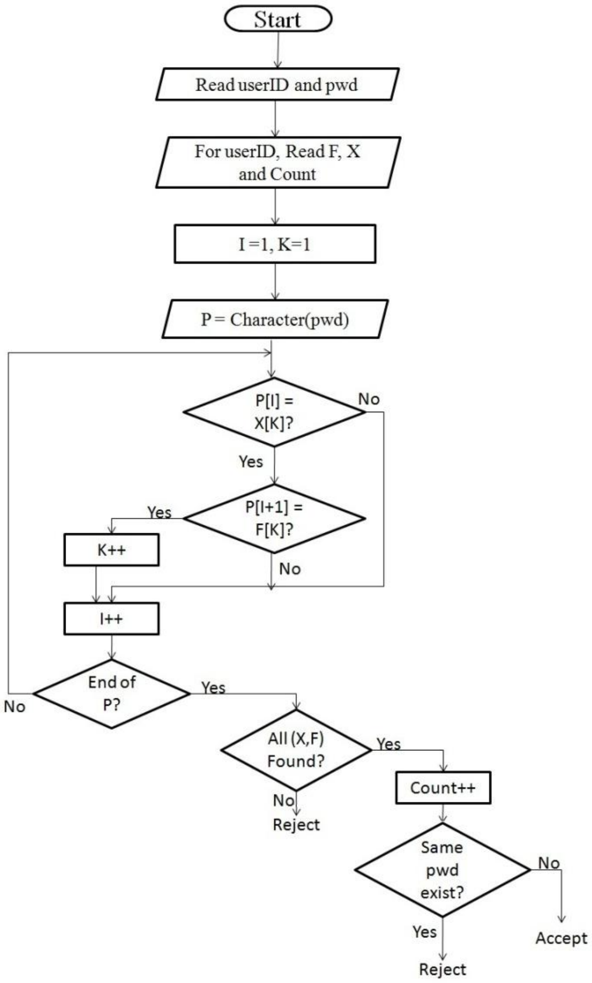

Fig 3: User Authentication

Fig 3 describes how the actual password gets extracted and the user will get authenticated. In order to understand the extraction process, let us consider the following example. For simplicity, let us consider all the characters are of numeric type.

Example:
Actual Password (F) = 4,2,7,8
Terminator set (X) = 6,3,5,1
Variable set (V) = any variable length string.

Note that set V is not specified by the user at the time of registration. Only F and X are known.

Now at the time of log in, user provides following variable length noisy password, containing variable noise, actual password and terminators embedded in it.

63462375692649636258569888845547532122375432566757
45643223676743255687986543285348518088553225689976
554445837438

At the server side, program traverse the string and check for first character of terminator set and whether the immediate character of subset of terminator is the subset of actual password but in sequence. The bold character shows the terminator set and the gray colored italic character shows the subset of actual password. If the pair (X, F) is found, the server will then check for next character pair. Once all the pairs are found, the server will permit the user to log in to the system otherwise reject it.

634623756926*4*963625856988884554753*2*12237543256675*7*
4564322367674325568798654328534851*8*088553225689976
554445837438

For every successful access to the account, a counter is maintained for each noisy password. The reason to maintain the count is that, user will not be able to log in to the system using same sequence of characters. Hence, this will protect the account of user, if any intruder captures the keystrokes. The algorithm for the password extraction is given below.

Algorithm 2 User Authentication

Require: userID (Username) and pwd (Noisy Password)

```
Fetch terminator set (X) and actual password (F) from database using userID as key
Initialize i □1, k □1,count □0
P □pwd
for all i such that i 6 Length(P) do
   for all k such that k 6 Length(X) do
         if P[i]_X[k] then
            if P[i + 1]_ F[k] then
                 k □ k+1
            end if
         else
              i □ i+1
         end if
   end for
end for
 if k _Length(X) then
    count □ count+1
    if pwd exist in database? then
          Unsuccessful Login
    else
        Successful Login
end if
else
   Unsuccessful Login
end if
```

5. CONCLUSION

Traditional static text-based password technique is the most common method used by the application for authentication. Another method is graphical method or image based method. But both the techniques are nonresistant to the shoulder surfing and also difficult to remember. In this paper, an alternate authentication technique is used to mitigate the attacks mentioned above. Since noisy password technique uses different password string, it has been proved resistant to the attacks like eves dropping, key loggers, Trojan attacks etc. In future, the Noisy Password technique can be combined with other authentication schemes. More experimentation on combining this technique with Biometric authentication system is to take place in future.

6. ACKNOWLEDGMENTS

I represent my sincere gratitude to Prof. K. V. Warkar, Assistant Professor, BDCE, Sewagram, for her constantly guidance throughout the work and support.

7. REFERENCES

[1] Mahto, D. and Yadav, D. K. 2015. Enhancing the Security of One-Time-Password using Elliptic Curve Cryptography with Biometrics for E=Commerce Application. Third International Conference on Computer , Communication, Control and Information Technology (C3IT), 1-6

[2] Chaudhari P. P., Hajare S., and Bhusare P. Feb 2015. Image Based Password Authentication. International Journal of Advance Research in Computer Science and Software Engineering. vol 5, Issue 2.

[3] Thenmozi C., Sathvi S., and Thamotharan B. Jun-July 2013. Two Level Authentication System. International Journal of Engineering and Technology. Vol 5, no. 3, 2036-2040.

[4] Manjunath M. Ahmad K. and Suchithra. March-April 2013.Security Implementation of 3-Level Security System using Image Based Authentication. International Journal Of emerging trends and Technology in Computer Science, vol.2, Issue 2, 401-404.

[5] Sediyono E., Santoso K. I., and Suhartono. 2013. Secure Login By Using One-Time Password Authentication Based on MD5 Hash Encrypted SMS. International Conference on Advances in Computing, Communication and Informatics (ICACCI), IEEE, 1604-1608.

[6] Alkhathbar K., and Mahmoud H. A. 2009. Noisy Password Scheme: A new One Time Password System. Canadian Conference on Electrical and Computer Engineering. 841-846, IEEE.

[7] Alkhathbar K., and Mahmoud H. A. November 2009. Noisy Password Security Technique. International Conference for Internet Technology and Secured Transactions (ICITST), 1-5. IEEE.

[8] Nitin, Sehgal V., Chauhan D. S., Sood M., and Hastir V. 2008. Image Based Authentication System with Sign-In Seal. Proceedings of the World Congress on Engineering and Computer Science.

[9] Wen-Chung Kuo and Yung-Cheng Lee. August 2007. Attack and Improvement on the One-Time Password Authentication Protocol Against Theft Attacks. Proceedings of the sixth International Conference on Machine Learning and Cybernetics, IEEE.

[10] Newman R. E., Harsh P., and Jayaraman P. 2005. Security Analysis of and Proposal for Image Based Authentication. International Conference on Security Technology. 141-144. IEEE.

[11] Weinshall D., and Kirkpatrick S. 2004. Passwords you'll never forget, but can't recall. In Proceedings of Conference on Human Factors in Computing System (CHI). 1399-1402. ACM.

[12] Harris J. A. 2002. OPA: A One-Time Password System. In Proceedings of International Conference on Parallel Processing Workshops (ICPPW'02). 25-29. IEEE.

[13] Dhamija R., And Perrig A. 2000. Déjà Vu: A User Study Using Images for Authentication. In Proceedings of 9th USENIX Security Symposium.