IJCSI International Journal of Computer Science Issues, Volume 14, Issue 6, November 2017
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org https://doi.org/10.20943/01201706.2934

Efficient Implementation of oPass User Authentication Protocol

Laiali Almazaydeh[1], Ketul Patel, Raul Timbadiya, Siddhartha Chauhan, Abiodun Adeleke and Khaled Elleithy[2]

[1] Department of Software Engineering, Al-Hussein Bin Talal University
Ma'an, Jordan

[2] Department of Computer Science and Engineering, University of Bridgeport
Bridgeport, CT, USA

Abstract

Nowadays, most of the web-based applications requires typing textual password to confirm one's identity to remote service. However, applying textual password for authentication purpose has considerable security attacks such as password stealing attack and password reuse attack. Therefore, various approaches are proposed for securing user authentication to login to a website. In this paper, we improve a user authentication system named oPass which referred to online password. The identity of the user will be authenticated through cellular phone which is used to generate a one-time session password, then transmit the encrypted message through short message service. With the proposed technique, a deeper user authentication is performed without revealing password to the untrusted computers.

Keywords: *opass; authentication; security; sms, textual password.*

1. Introduction

User authentication is a process that allows a device to validate the identity of someone who accesses the information and a network resource. Traditionally, textual password is the most basic form of user authentication. Widely deployed web applications require user password in order to facilitate their services usage, such as, e-commerce, e-mail, cloud computing, and social networks. However, applying textual password for authentication purpose has considerable attacks. One of these attacks is referred to as the Password reuse attack [1], [2], as it is known that the user tends to reuse password across 3.9 various websites on average [3]. Thus, once the attacker compromises that password, then she / he will use the same password for each website to access the related sensitive information of the user. Another crucial attack is Password stealing attack. Many malicious software aims to impersonate users' identities to steal the personal and financial information. Phishing and malware are the most common password stealing attacks, in 2010, APWG's report [4], indicated that there are 97 388 unique phishing websites detected at the second season of that year.

Up to now, researchers have investigated two other techniques in the user authentication procedure instead of textual password. First, various graphical password methods were developed in [5]-[9] to address textual password recall problem. Second, password management tools were used in [10]–[12] to address textual password recall and reuse problems. However, both techniques are not yet work well to be widely implemented in a fully secured system [13]-[17].

In order to improve the user authentication procedure, the researchers have investigated for some time three-factor authentication instead of depending only on textual password authentication. To prove the identity through the three-factor authentication, the user provides a password and pass code, and scan a biometric feature. Combining three-factor authentication in such a way is a comprehensive protection mechanism but it is costly [18]. Therefore, combining two-factor authentication is cheaper and more practical than three-factor authentication.

In this paper, we improve a user authentication system named oPass which referred to online password. The proposed system involves cellular phone which is used to generate one-time session password then transmit the encrypted message through short message service (SMS), thereby, gaining a deeper user authentication without revealing the password to untrusted computers.

The rest of this paper is structured as follows. Section 2, elaborates a variety of user authentication techniques. Section 3 identifies the problem. Section 4 presents details on the proposed approach of the paper. Section 5,

demonstrates results of the proposed approach. Finally, Section 6 concludes this paper.

2. Related Works

Textual passwords are facing many problems like weak passwords, password reuse and many more. Many works were developed to focus on overcoming the weak password problem. Numerous researchers like Goldberg el. al. in [19] suggested using the graphical password instead of textual password. The authors had different options in using graphical password like using doodles or using a series that of random art images or the images of people's faces. The benefit of these systems is that the images can be easier to be recognized by the people or to remember them instead of remembering textual password. Moreover, these passwords can be selected more strongly than the weak textual password that can be easily cracked. In contrast, Bunnell et al. have focused on textual passwords, looking at recall rates for different methods to generate and associate these passwords [20].

The work in [21] is an alternative to the textual based password system. According to this work, the graphical password was better than textual based password to prevent brute force or dictionary attacks. However, the graphical password had much vulnerability. The graphical password was easy as compared to textual password but was easier to compromise the password too. The traditional attacks were not good to crack the graphical password as to crack textual based password but simple attacks like shoulder surfing is the easiest way to know the password. Thus, it was concluded that there are a lot of studies have to be done to improve the graphical password strategy to replace it instead of textual based password.

In 2012, a technique was proposed in [22], called oPass in which it was suggested using SMS, a text based communication service of telecommunication system, to transmit password instead of using the internet channel. SMS is considered the most secured and successful data transmission channel of telecommunication system [23]. In this system the authors have assumed that the user's cellular phone will be connected to the machine that the user wants to access and then the user will try to use the internet and request access to any website. Once the user makes an access request, the server will send some information to that machine which will be received by the user's cellular phone and then, the cellular phone will prompt a dialogue box for the user to enter the password. This password will then be sent to the server from the cellular phone directly. Here the authors also have assumed that the telecom service provider will take part in this process. Now the server will receive the password and then it will verify the password and the request will be completed and the user will be given access based on the result of the request matching.

3. Problem Identification

Various techniques like key loggers, phishing web pages etc. are used to hack the password which makes it difficult to secure passwords. Also, using the same password on different web sites causes domino effect [1]. There was no existing system to solve both password stealing and password reuse attacks simultaneously, until oPass method was presented. The proposed authentication method uses cellular phone to send password through text message which makes the password safe compared to the existing methods, as the SMS channel is most secured channel for data transmission. One reason for the channel being safe is that SMS channel is an out of band channel than internet channel. Thus, the password security is increased as compared to existing system. The threat of phishing attacks and Key loggers is reduced which can make users free from the worry of password stealing. Also the user has benefit of using same password across different websites.

oPass method was proposed by authors in [22]. They also carried out some experiment and achieved good results. Even though the proposed oPass system is secured, there are some minor drawbacks. The issue is that the user had to type the password on the cellular phone and send it using the text message service. Here there are chances that the users do not delete the sent password. In the case the user's cellular phone was stolen or used by someone, then the password will no longer remain safe. Even if someone standing nearby keeps an eye when the user sends the password text message, in this case the password is no longer secured.

To overcome the aforementioned drawbacks, we can encrypt the password that is being sent through SMS. We can create an application that will be installed in the user's cellular phone and that application will generate the encrypted password. This password can be used to send through the SMS service. All we need is to just convert the readable string to unreadable format so that it cannot be easily compromised. So, for that we can provide the application with several inputs like name, birth date and password. The application will then process this information and use this information to generate the encrypted password. The user then copy that output and send that through SMS.

On the server side, the website will also have the same information that is the name, birth date and the password. The server will also run the same code to generate the

encrypted password. But this process will be done once the user has requested to use the service provided by the server.

Once the server creates the encrypted password, it will then allocate some time stamp. This will be a time period after which the server will discard the request. So the user will need to send the password before this time stamp expires. Once the server receives the message, the content of the message will be compared to the password generated by the server. If they match then the server will allow the user to use the services, otherwise the server will simply discard the request and inform the user requested service and will also send a notification to the user to whom the account belongs.
Since we are using cellular phone the do the encryption, we need some small and very less complex mechanism to encrypt the password. All we want to do is to convert an easily readable string to complex string. So we can create a general string which includes the first name, last name and the password of the user. Once the string is created, the string characters can be shuffled. To do this we can use the date of birth of the user. Using the date of birth we can get a number which will define the positioning of the characters. Once the characters are shuffled, we can still shuffle it more and then convert these characters to integer. To do this we can convert the characters to their equivalent ASCII values. Once the characters are converted to string it will make it difficult to determine the original password. This method is not very complex so it will be easy to implement as an application.

4. Methodology

In this system we start with the registration phase then the login phase and recovery phase if required. Here the user first needs to register on the website and also register his cellular phone there to make it a token of authentication. This token can be used with the password as a means of authentication. The detailed process is discussed below.

1.1 The Registration phase

In this phase the user creates an account on the website through any kiosk and registers on that site giving his detailed information and also provides the cellular phone number. The website server then sends a link to download the application on the cellular phone. Once the application is installed, the user will be asked all the information that he entered while creating the account. This information will be stored in the database of the application. Here the user will provide details like name, birthdate and password. Once the details are entered, the application will generate a password and will send that password to the server through SMS. The server will run the same encryption process and verify the password that it received along with the cellular phone number. The server will generate the password and match that with the one that arrived in SMS. If the passwords matched then the user account will be created successfully, otherwise the server will send a message notifying that the passwords did not match. This will continue till the password matches. Each user will have one account and will be identified using the user name and the cellular phone number. One cellular phone number will not be used to create another account on the same website.

1.2 The Login phase

Once the user is registered on the website through the above process, then the user can use the method to login on the website. In this phase the user is required to make a request for login on the website. Here the user will just need to enter the username on the web page and make the request. Then the user uses his cellular phone to generate the password. The user will open the application and request the password. The application will encrypt the data stored in the database and provide a password. Then, the user will copy that password and send it to the desired server through SMS. On the other hand, the server will process the user details and run the same encryption that runs in the application. The server will also generate the password and keep it ready to match with the password received in SMS. Once the server receives the SMS, it will first check the cellular phone number and verify that. Once the number is verified the server will match both the passwords. If the passwords do not match then the server will return a message informing that the password is incorrect and will provide one more try to send the password. Here the server will wait for some time period. In that time period if the SMS is not received then the server will discard the login request. Thus the user will have to be quick in sending the password. If the password match fails then the server will extend the timer and give one more try to the user to send the correct password. This will happen twice and still if the user fails to provide the correct password then the server will block the account temporarily and notify the user on his cellular phone. If the passwords were same then the user grants the access on the machine that he requested access.

The application has the details of the user like the first name last name password and the birthdate of the user. So when the user makes a request for the password, the application will use all this information to generate a string that can be used for encryption. Figure 1 shows part of encryption step.

In this step the name and the password will be stored in a string combined. The application will produce the sum of the date of birth and the month of birth and generate a

number. This number will be less than 15. If it goes above 15 then both the digits will be added again and generate a smaller number. Now this number will be used to place the characters in different locations. The first letter will go on the first place then the second character will be places after leaving the space of the size of number. For example in the figure 1 the number is 10 so the character 'B' will be places at the 10th position after 'A'. In this way all the characters will be placed. Once it reaches the last position it will come back to the first position and continue counting from there. The position counter will only count the empty space. Means the total size in the example is 17 so these many blocks will be created to store characters and all the characters of the generated string will be placed within this space. Once the string is generated it will separate the string into small blocks of the size of the name. This is shown in figure 2.

Here the name size was 4, so the whole string was portioned into different blocks of size 4 each. The last block has just one character as the string was not of the size that is multiple of 4. Now this blocks will be merged into one blocks two at a time. So the first two blocks and the third and fourth blocks will be merged. In this merge the first character of block 1 is taken then the first character of block 2 is taken in this way all the characters are merged in one block from two blocks. Now it will merge the next two blocks after step 1 merge. In this merge the character choosing is different than the step 1 merge. The first character is taken from block one and the second character is taken from block two but in reverse order. That is the first character is character one of the block 1 and the second character is the last character f block 2. And in this last step all the remaining blocks will be merged by just appending all blocks together. These merged blocks will again form a string of characters. This string of characters

will be converted into a numeric form which will be difficult for a normal person to understand. So the final step is to generate the ASCII value of each character. This ASCII value is then used to send to the server. Figure 3 shows the final step.

After that, the application will ask the user whether he wants to change the password or not. Here if the user changes the password then he will have to do the same on the website. Since the user is already logged in the user can easily do this step. Or just the user can deny changing the password.

1.3 The recovery phase

In this phase the user can do the several actions like blocking the account temporarily in case if the cellular phone is stolen or if he receives the message from the server without requesting the access. The recovery option will be available on the website or the user can send a message to the server saying block the account temporarily.

5. Simulation Results

We implemented the encryption algorithm as an experimental application. The algorithm was implemented using C++ on the windows platform using visual studio software. The algorithm takes the users birth date and month first. Then it calculates the sum of the birth date and stores it. Then the user input the First name, Last name and the password. It stores this information and generates a string combining all three attributes. Then it starts the encryption process, and finally it generates the encrypted password string. The user will need to copy this string and send it through the SMS to the server. Figure 4 shows the output screen of this application.

As mentioned, the last string is the encrypted password string that will be provided to the user when the application runs. This is a prototype of the application.

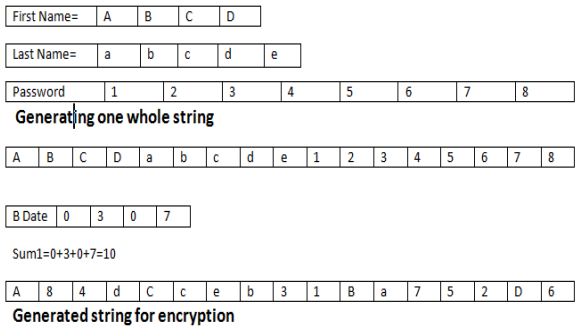

Fig. 1. Generating string for encryption

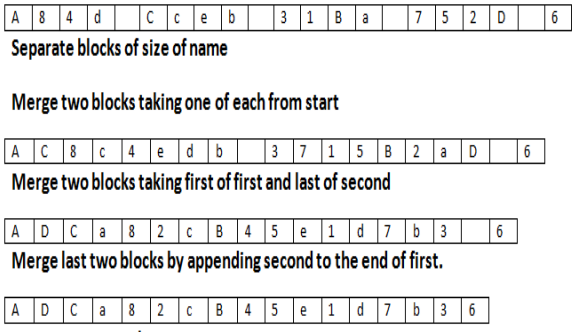

Fig. 2. Separation of string and merging the blocks

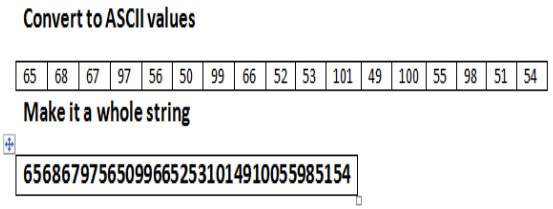

Fig. 3. Generating ASCII values

Fig. 4. Application results output

6. Conclusion

In this paper, we proposed encryption approach to the message that will be sent from the user cellular phone to the server through SMS. This will help in adding security to the authentication system proposed by Hung-Min in 2012 [22]. We assume that telecommunication companies will participate in this process and will provide a unique number to the servers. When the user wants to use the service of any website, he will request login from the kiosk and will send the password through the cellular phone in SMS. Here the user will first launch the application which will provide the encrypted password. The user needs to copy the password and send it through SMS. On the server side the server will also process the password and generate the encrypted password. Once it receives the SMS it verifies and provides the access accordingly.

The design principle of this method is to make user free from remembering long complex passwords. Using the proposed method the user need to remember one password of his choice and few security questions that are easy as the user have a basic idea of the answers as it relates to him. Also the user is free from the threat of password being compromised by several attacks like key logger and phishing attacks.

To design the application, a simple encryption technique is used instead of the complex algorithms like blowfish, AES, etc. This will be better as the application has to run on the cellular phone so it will take less processing time and memory. An prototype application was developed to demonstrate the proposed encryption technique which had good results as it quickly generated the output once it received the inputs. The overall conclusion is that, the oPass system with password encryption proves to be efficient and more reliable than the current authentication process, as it eliminates several drawbacks and threats.

References

[1] B. Ives, K. R. Walsh, and H. Schneider, “The domino effect of password reuse,” Commun. ACM, vol. 47, no. 4, pp. 75–78, 2004.

[2] S. Gawand E. W. Felten, “Password management strategies for online accounts,” in SOUPS ’06: Proc. 2nd Symp. Usable Privacy . Security, New York, 2006, pp. 44–55.

[3] D. Florencio and C. Herley, “A large-scale study of web password habits,” in WWW ’07: Proc. 16th Int. Conf. World Wide Web., New York, 2007, pp. 657–666.

[4] Phishing Activity Trends Rep., 2nd Quarter/2010 Anti-Phishing Working Group [Online]. Available: http://www.antiphishing.org/

[5] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, “The design and analysis of graphical passwords,” in SSYM’99: Proc. 8th Conf. USENIX Security Symp., Berkeley, CA, 1999, pp. 1–1, USENIX Association.

[6] A. Perrig and D. Song, “Hash visualization: A new technique to improve real-world security,” in Proc. Int.Workshop Cryptographic Techniques E-Commerce, Citeseer, 1999, pp. 131–138.

[7] J. Thorpe and P. van Oorschot, “Towards secure design choices for implementing graphical passwords,” presented at the 20th. Annu. Computer Security Applicat. Conf., 2004.

[8] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, “Passpoints: Design and longitudinal evaluation of a graphical password system,” Int. J. Human-Computer Studies, vol. 63, no. 1–2, pp. 102–127, 2005.

[9] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, “Design and evaluation of a shoulder-surfing resistant graphical password scheme,” in AVI ’06: Proc. Working Conf. Advanced Visual Interfaces, New York, 2006, pp. 177–184.

[10] B. Pinkas and T. Sander, “Securing passwords against dictionary attacks,” in CCS ’02: Proc. 9th ACM Conf. Computer Communications Security, New York, 2002, pp. 161–170.

[11] J. A. Halderman, B. Waters, and E. W. Felten, “A convenient method for securely managing passwords,” in WWW ’05: Proc. 14th Int. Conf. World Wide Web, New York, 2005, pp. 471–479.

[12] K.-P. Yee and K. Sitaker, “Passpet: Convenient password management and phishing protection,” in SOUPS ’06: Proc.

2nd Symp. Usable Privacy Security, New York, 2006, pp. 32–43.

[13] S. Chiasson, R. Biddle, and P. C. van Oorschot, "A second look at the usability of click-based graphical passwords," in SOUPS '07: Proc. 3rd Symp. Usable Privacy Security, New York, 2007, pp. 1–12.

[14] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in CHI '09: Proc. 27th Int. Conf. Human Factors Computing Systems, New York, 2009, pp. 889–898.

[15] J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and thememorable space of graphical passwords," in SSYM'04: Proc. 13th Conf. USENIX Security Symp., Berkeley, CA, 2004, pp. 10–10, USENIX Association.

[16] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," in SS'07: Proc. 16th USENIX Security Symp. USENIX Security, Berkeley, CA, 2007, pp. 1–16, USENIX Association.

[17] P. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," IEEE Trans. Information Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.

[18] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proc. IEEE, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.

[19] J. Goldberg, J. Hagman, and V. Sazawal. Doodling our way to better authentication. In Proc. of Ext. Abstracts CHI 2002, pages 868{869, New York, NY,USA, 2002. ACM Press.

[20] J. Bunnell, J. Podd, R. Henderson, R. Napier, and J. Kennedy-Moffat," Cognitive, associative and conventional passwords: Recall and guessing rates," Computers and Security, vol. 16, no. 7, pp. 641-657, 1997.

[21] X. Suo," A Design and Analysis of Graphical Password," master thesis, 2006.

[22] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks", IEEE Transactions On Information Forensics and Security, Vol. 7, No. 2, pp.1556-6013, 2012.

[23] I. T. Report, ITU Internet Rep. 2006: Digital.Life [Online]. Available:http://www.itu.int/