Providing Security to User Data using OTP and Image CAPTCHA

K. L. R. S. Himaja [*1], Mrs.T. Sri Lakshmi [*2]

* PG Student, CSE Department, PVPSIT College/JNTUK University, Vijayawada, A.P, India

*Sr. Asst. Professor, CSE Department, PVPSIT College/JNTUK University, Vijayawada, A.P, India

Abstract— *Data Security is that preventing from unauthorized disclosure and modification. The basic and old method of computer authentication is to use alphanumerical usernames and passwords. This method has been shown to have important drawbacks i.e., These passwords are prone to be stolen and vulnerable to different types of attacks. Then Captcha technology came into existence but again it fails as an individual. Then after graphical password came into existence and has its own drawbacks. This paper provides OTP and image captcha together which provides high security.*

Keywords— *Captcha, Otp, User Authentication.*

I. Introduction

Security is a critical part of any Web applications. Web applications by definition allow users access to a central resource — the Web server — and through it, to others such as database servers.

Working with security requires that you understand these fundamental security concepts:

Authentication confirms user identity. Whether they are genuine users are not depending on username and password.

Authorization is the process of granting or denying access to resources for specific users. however are vulnerable to a variety of attacks. Human memorable passwords are making brute force and dictionary attacks feasible.

Passwords are a worldwide familiar method of user authentication. There are mainly two types of passwords:

- Static password
- Dynamic password

Static passwords are traditional human memorable passwords that are only changed if necessary. These passwords are making brute force attack and dictionary attacks vulnerable. Static passwords highly susceptible to cracking because passwords used will be cached on the hard drives.

Dynamic passwords came into existence so as to solve the existing static passwords problem. Dynamic passwords are those that change every time the user logs in, known as One Time Password (OTP). An OTP has set of characters that can act as identity for only once. Once the password is used, it can no longer used for any further authentication. Even if the attacker hacks the password, its most that it was already used once, as it was being transmitted, thus it is useless for the attacker.

II. . Literature Survey

In this proposed model provide high security to user data using two authentication techniques, one is by using session password and another is Image Authentication Technique.

One Time Password(OTP): The main concept of using OTP is that to overcome attacks that are possible due to the use of normal static passwords. some of the attacks are:

Key logging that gather sensitive information from users computer, especially their passwords. In OTP the user are able to log into web service only with the password that is randomly generated and sent to the mail.

Phishing attacks are often launched for stealing users passwords by cheating users when they connected to duplicate websites. This can also be overcome by using OTPs, that allow the user to login to the site without revealing the passwords.

Prevention of reused passwords is another advantage of using OTP. The password is different every time when the user login, user no need to remember the password for login and it will be difficult for the hacker to hack the password. Even if it is tracked it is useless as the is used already by the user.

Techniques in Generation of One Time Password

One time password can be generated in any of the two ways:

- Time-synchronized OTP
- A counter-synchronized OTP

In **Time-synchronized OTPs** the user should enter the password within a certain amount of time else session expires and another OTP must be generated.

In **Counter-synchronized OTPs**, a counter is set between the client device and the server. The counter is increased each time an OTP is requested.

Modes of OTP Delivery

Text messaging: A common technology used for the delivery of OTPs is text messaging. Because text messaging is a ubiquitous communication channel, being directly available in nearly all mobile handsets and, through text-to-speech conversion. Text messaging has a great potential to reach all consumers with a low total cost to implement. However, the cost of text messaging for each OTP may not be acceptable to some users.

Instant Message Services and Email: These services are almost common and the cost of using them is negligible.

Mobiles: A mobile phone keeps costs low because a large customer-base already owns a mobile phone for purposes other than generating OTPs. The computing power and storage required for OTPs is usually insignificant compared to that which modern smart phones typically use. Mobile phones additionally support any number of tokens within one installation of the application, allowing a user the ability to authenticate to multiple resources from one device.

Web Based Methods: Authentication-as-a-service providers offer various web-based methods for delivering one-time passwords without the need for tokens.

IV.PROPOSED SYSTEM

In this paper, we propose a user authentication protocol called one time password (OTP) which is sent to the specified user e-mail. We use MD5 algorithm for generating the OTP. And in addition to OTP another authentication is done called as Image Captcha.

Image Captcha At the time of registration to the site it requests the user to select an image. Whenever the user tries log in to the site it asks the username and password then after authentication has to select the image that was selected at the time of registration, from a group of pictures displayed. This type of technique is called picture-based recognition technique. If selects the wrong image then immediately the account will be blocked, to release the account from blocking a request should be sent to the admin.

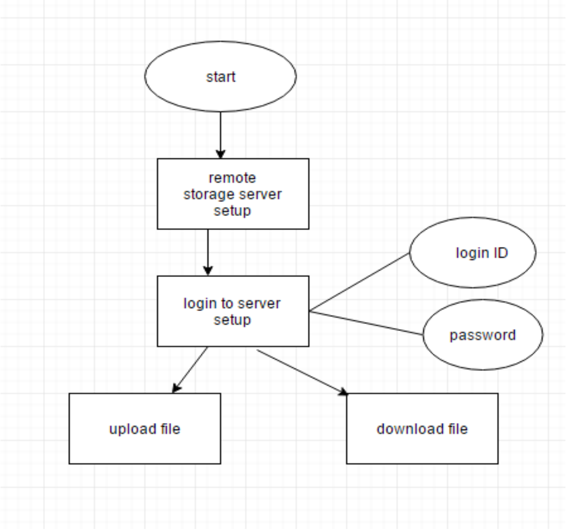


Figure 1: Data Flow Diagram of proposed model

The above figure shows the data flow diagram of the proposed model in which at the start stage the remote server has to be setup. Then the users can login to that web server using image captcha and OTP. The following process is done at each module.

Data Upload In this Module the registered user has to choose one file from the system and then upload the file. Then an OTP is generated and sent to mail that is specified at the time of registration. If correct OTP is typed then file is uploaded will be stored in the server else the account is blocked.

Data Download Now, the client can download the file. The user can download the file only if he is granted access. The Access is permitted only of the user types the correct OTP that was sent through the e-Mail. If correct OTP is typed then download will be done.

V.IMPLEMENTATION

Here we use MD5 algorithm for generating One Time Password. MD5 algorithm takes input message of arbitrary length and generates 128-bit long output hash. MD5 is commonly used hash algorithm.

MD5 Algorithm has a total of five steps:

Step 1: Padding bits should be appended

The message is extended so that the length will be equal to 448, modulo 512. This message is extended to be a multiple of 512.

Step 2: Append length

The message should have a length of multiples of 16.

Step 3: Initialize buffers

Four buffers has to initialized P, Q, R, S Each Of 32 bit.

Word P: 32 42 a1 76
Word Q: 21 69 ef 26
Word R: 56 72 86 f1
Word S: 91 02 69 ae

Step 4:

We perform these four functions to each round. And produces 32 bit word

A(F, G, H) = FG v NOT(F) H
B(F, G, H) = FH v G NOT(H)
C(F, G, H) = F XOR G XOR H
D(F, G, H) = G XOR (F v NOT(X))

Step 5: output

The message digest produce an output P, Q, R, S. Starts with lower byte as P and with S as high order byte.

VI.RESULT AND DISCUSSION

Here in below figure where the user selects the image that was selected at the time of registration. The account is blocked if selected the wrong image, then account is in blocked state until admin again activates it.

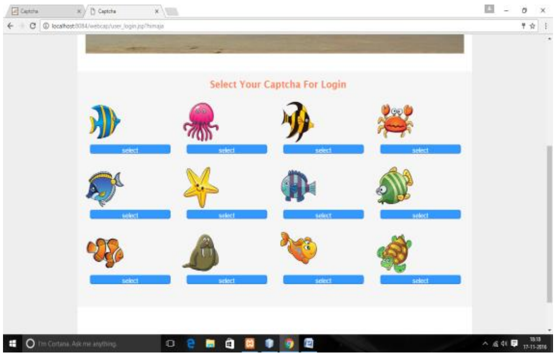
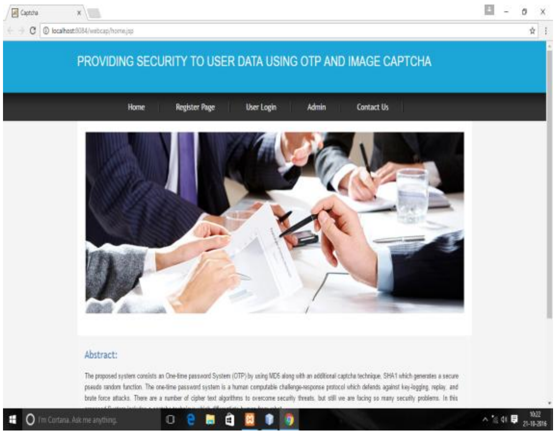

Captcha
Captcha
localhost:8084/webcap/user_login.jsp?himaja
Select Your Captcha For Login
select
select
select
select
select
select
select
select
select
select
select
select
I'm Cortana. Ask me anything.
10:18
17-11-2016

Figure 2: shows the image selection at the time of login


Captcha
localhost:9084/webcap/home.jsp
PROVIDING SECURITY TO USER DATA USING OTP AND IMAGE CAPTCHA
Home
Register Page
User Login
Admin
Contact Us
I'm Cortana. Ask me anything.
10:22
21-10-2016

Abstract:

The proposed system consists an One-time password System (OTP) by using MD5 along with an additional captcha technique. SHA1 which generates a secure pseudo random function. The one-time password system is a human computable challenge-response protocol which defends against key-logging, replay, and brute force attacks. There are a number of cipher text algorithms to overcome security threats, but still we are facing so many security problems. In this

VII.CONCLUSION

When compared to previous techniques that which does not have that much capability to secure password from hackers, this system provides security to user account by using both the OTP and Image CAPTCHA. The OTPs is dynamic password that changes for each session providing high security for banking, applications etc., Image authentication technique is where it provides an extra security to the web service.

Figure 3:download page where OTP is generated

REFERENCES

[1] 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, April 2012.

[2] Prof. Bogiri Nagaraju Computer KJCOEMR Pune, Maharashtra,"Authentication Schemes for Session Passwords using Hybrid and Paired based Techniques", *Multidisciplinary Journal of Research in Engineering and Technology Volume 1, Issue 2, Pg.175-182*

[3] Michel Abdalla , Emmanuel Bresson, Olivier Chevassut Provably Secure Password-Based Authentication in TLS March 21–24, 2006

[4] Introduction to Basic Security Concepts by Robert H. Williams III, 2007.

[5] Chun-I Fan, Chien-Nan Wu, Chi-Yao Weng, Chung-Yu Lin Active One-Time Password Mechanism for User Authentication

[6] Introduction to Basic Security Concepts by Robert H. Williams III, 2007.

[7] A Survey on Different CAPTCHA Techniques Volume 3, No.2, February 2014 Advances in Computer Science and Technology

[8] R. Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Comput. Surveys, vol. 44, no. 4, 2012.

[9] Y.Yesu Jyothi, D.Srinivas, K.Govindaraju, THE SECURED ANTI PHISHING APPROACH USING IMAGE BASED VALIDATION, International Journal of Research in Computer and Communication Technology, Vol 2, Issue 9, September -2013