International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 12, December - 2013

Two Step Based Multi-Web Authentication System

Ms. Phani Deepthi .Y [(1)]
Student (M.Tech.)
deepthiphaniy@email.com
CSE Department
BVRIT, Narsapur.

Mr. P. Bhaskara Rao [(2)]
Assistant Professor
CSE Department
BVRIT, Narsapur.

Abstract

Two Step based Multi-Web Authentication System is an open web based authentication system which uses the advanced security authentication system with strong encryption techniques and 2 mode authentication for multiple web portal authorizations. The Two Step based Multi-Web Authentication System uses the advanced encryption with strong symmetric enabled encryption to enhance the security to the web portal, it mainly delivers the one time password or codes to the web portal user with the multiple framework tokens with unique keys which runs on the standalone webserver or the desktops. It uses both the two keys such as public key and private keys in order to generate the passcode on the end-user devices. It uses the static passwords and dynamic passwords for generating unique code for the web portal authentication. Web server with sms support and SMTP support, it enables the two step authentication and it sends the passcode over sms gateway to the mobile devices and it also sends the passcode to the email address for 2 step verification.

1. Introduction

Two Step based Multi-Web Authentication System is a verification mechanism of the multiple web authentication which is relatively easy to access using the advanced verification system to understand the web security system. It uses the advanced passcode generation technique in order to begin the key optimization in terms of private key and public key for every end user that is issued with a random unique key to the user end devices. Both the multiple web servers and multi authentication system as the client which uses the advanced encryption in order to copy the unique key and that generates the random key and it sends to the user. It is assumed that both the web servers uses the multi-authentications followed by the two factor authentication modes with the client which can synchronize the user clock settings which is automatically saves on the webserver. Whenever the user undergoes the website login process and the client automatically takes the server integrated current web time stamp to the previous mode which frequently occurs for every 30 seconds interval in a authentication webserver. The web authentication client also makes the unique and random combinations of the multiple unique keys along with the time stamp and session mode of the authentication system.

2. Requirements

- Requires a standalone Linux web server which supports open source technologies
- Webserver enabled with SMTP Support
- Webserver enabled with Short Message Service Support

- Webserver enabled with two factor authentication Support
- Webserver enabled with rubyonrails Support
- Webserver with Network Operator Support
- Web portal with Session Tracking Support
- 24 x 7 Internet Connectivity
- Push mail support and Push text(Short Message Service) Support

3. Two Factor Authentication Technology

- It is a better solution for web portal advanced security authentication system which is more secure and flexible way of advanced authentication system is also known as the two factor or the two step multi web authentication with the advanced strong authentication, which is mainly based on delivering the one time unique codes and the one time passcodes to the user's mobile device or to the user's email id.
- It is mainly done with the silent authentication process which has a quite advanced security threat management system. It also has many benefits with the unique pass code generation which cannot be guessed, cannot be misused, cannot be generated illegally, easy to be written down and cannot be stolen easily and is very secured.
- In the other hand the main benefits is that it has integrated with the strong authentication and verification system that when every web portal user has the advanced feature that which can be included with the unique token which will be sent to the end-user device.
- This feature is not expensive and it is open source that it can be integrated on any website or web portal and it also supports HTTPS (Secure Socket Layer).
- Fortunately, many user devices which are capable of running the scriptlets can make the use of two step verification.
- It stands with the reason for making the use of two step authentication system as the unique authentication passcode token. It is the very secure way to authenticate the multi-web portal.

4. Architecture

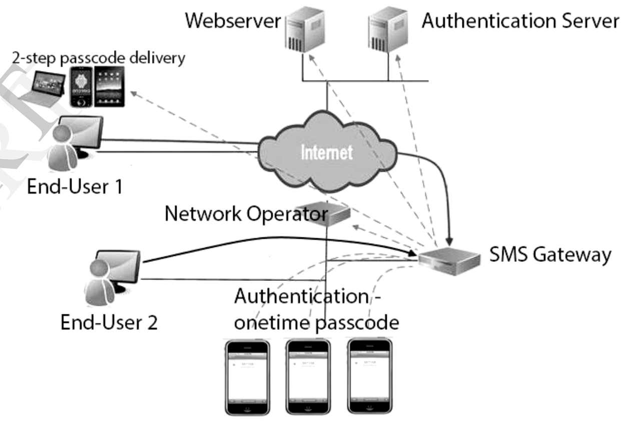


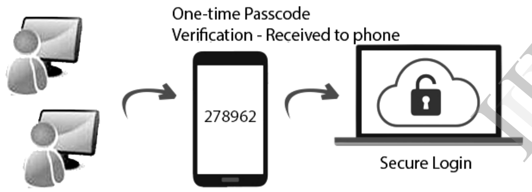
Figure: 1 Architecture – Two Step based Multi-Web Authentication System

Two Step based Multi-Web Authentication System is an open source based authentication system which is capable of generating the Onetime passcodes for logging into the web portal, Background server generates the passcodes and it delivers to the end-user device with the help of sms gateway.

Webserver connects to the SMS Gateway to the network operator and it delivers the code, the code will be identified itself in the web portal with the help of two factor authentication server which allows that it can be used in the most Multi-web environments using the 2-step authentication system.

Two Step based Multi-Web Authentication System uses the unique code generation randomly with the help of string of the unique keystrokes passcode which is typically sent to the authentication server via the network port over the sms gateway and delivers to the server with the input dialog of the authentication server and the sent code will be generated and processed to the server to the web portal or web host applications for the verification process.

5. How it Works?



- Two Step based Multi-Web Authentication System uses the string authentication which comprises with the both public key and the private key strings for identifying the generated passcodes in the authentication server which is particularly sent to the end-user device which is followed with the static one time passcode generation.

- There are many ways for authenticating on the web portal or website with the different options available for the end-users and also for the developers, it is supported with more than one passcode so, that users have the choice of authenticating on the web either 2-step verification with onetime passcode or direct authentication on the web.

- The main aspect is most common and the simplest way of authenticating and is to use whenever required to authenticate based on the time based onetime passcode generation.

- One of their main idea is to authenticate with the regular username and the regular password with the help of two factor verification system, users also have to input or enter the 5 digit passcode that always changes within every 45 seconds based on the token sessions.

- User token system to the token authentication server will generate the random and the unique token with the secret key and the user will be able to generate the valid code or the one-time passcode for the user accounts.

- It is safest and secure way of authenticating the login system. It integrates the 256-bit encryption AES into the authentication system, which is supported by authentication server which provides the advanced security.

- The passcode can be easily verified by the authentication server with the help of unique code identification system, whenever the server identifies the current time it automatically authenticates with the login system which uses the secret key and the secret PIN for identification of the end-user.

- In order to compensate with the authentication server time with the multiple differences which also enables the authentication webserver to accept the entered passcodes for 4 times within the time session of 3 minutes in the server authentication system.

- Each token will be generated randomly with the different time offsets which can also be easily specified for the each end-user with the help of the token-passcode identification system on the authentication server of that particular web portal.

- All the generated passcodes will be accepted for twice. After the 3 successive failures in the authentication system attempts, it blocks the user automatically and rejects whenever that particular user tries to login into the portal. 2-step Multi-Web Authentication System is totally based on two factors, one is by the passcode pin and is by the backup code secret passcodes.

6. Conclusion

Two Step based Multi-Web Authentication System is the two step based authentication which adds the two different additional layers to the security system on the multi-web portals by integrating the two steps or two factor based verification to the user login management system. It also adds the second factor which is typically generates the unique codes and sends to the user mobile device or user devices. The two step or two factor authentication and verification system avoids the security threats and blocks the attackers from accessing the user accounts.

We hereby conclude that, Two Step based Multi-Web Authentication System open source application framework can be implemented on any web portal or website for additional security, it adds the additional security layer on the multi-web.

References

[1] JohnArmington, PurdyHo, “A Dual-Factor Authentication System Featuring Speaker Verification and Token Technology" Published in year 2003, Vol2688, pp128-136.

[2] HaiyangSun,JianYang,YanchunZhng,XinWang, "Authorization Policy Based Business Collaboration Reliability Verification" Published in the year 2008, Volume5364, pp579-584.

[3] IngoMWeber, "Verification of Annotated Process Models" Published in the year 2009, Vol40, pp97-148.