Validation of One-Time Password (OTP)

Sachin Kumar Maurya[1], Sneha Ambhore (Guide)[2]

Abstract **-** The purpose of a one-time secret (OTP) is to form it tougher to realize unauthorized access to restricted resources, sort of a laptop account. Traditionally static passwords will additional simply be accessed by Associate in Nursing unauthorized unwelcome person given enough tries and time.

By perpetually sterilization the secret, as is completed with a one-time secret, this risk is greatly reduced. In this article, we tend to propose new secret technologies. The proposed system attempts to alleviate the problem of shoulder surfing or descent by making the playback of the password unnecessary.

Each time the user is completely different from the secret record. The noisy password consists of several parts, and the actual password and extra noise are thoroughly studied, and each time the user wants to authenticate themselves, a different password is generated. The beep component area unit has been tested to protect against any hacking attacks. Experimental results offer smart indication of the benefit of utilization of the new system with low error rates that may be increased by time.

Keywords *- component; formatting; style; styling; insert (key words)*

I. INTRODUCTION

Area unit 2 entities within the operation of the OTP one-time word system. The generator should manufacture the suitable one-time word from the user's secret pass-phrase and from information provided in the challenge from the server.

The server must send a challenge to the generator containing the appropriate generation parameters, must verify the received one-time word, must store the last valid one-time word it received, and must store the corresponding one-time password sequence number. The server must also promote changes to the user's secret passphrase in a secure manner.

The OTP system generator passes the user's secret password through multiple iterations of the secure hash and the seed received from the server as part of the challenge to provide a one-time password. The number of times the secure hash performs an iteration is reduced once after each successful verification. Therefore, a unique sequence of ciphers is generated.

The server validates the one-time password received from the generator once by computing a secure hash function, and compares the result to the previously accepted one-time password. Leslie Lamport first proposed this method. Password-Based Authentication Methods In password-based authentication protocols, two entities share a common password beforehand and use it as the basis for authentication.

Password authentication methods can be classified into two types: weak password authentication methods and strong password authentication methods. Weak password schemes have less computational overhead when compared to strong password schemes. In weak authentication, a password is associated with each entity. Passwords are usually 6 to 10 characters that users can handle in memory. On the other hand, strong authentication proves that only entities can be proved to other entities.[1]

Password Authentication Protocol (PAP) - Point-to-point protocol uses password authentication protocol to validate users before granting them access to server resources. All network OS remote servers support password authentication protocol. PAP is vulnerable because it sends unencrypted ASCII passwords over the network. PAP is recommended if the remote server does not support a stronger authentication protocol like CHAP (Challenge Handshake Authentication Protocol).

PAP authentication scheme, consists of two steps:

a) Authentication Request: In this, the user name and the password are sent by an Authenticate-Request Message at the initialization of the device.

b) Authentication Reply: Now the responding device looks at the name and password at the same time and decides whether to accept the initiating device and set up the link or to reject the link for the differences that had occurred. In such cases, it sends back an Authenticate-Ack and if not it sends an Authenticate-Nak respectively.

Password Authentication Protocol (PAP) Authentication Password Authentication Protocol works using the exchange of a request containing name and password information, Response indicating whether the authentication was successful.

II. VULNERABILITIES FOUND

www.mrshareef.com This website is an online shopping portal that allows users to create accounts with any mobile number and email address.

Also the details can be fake like invalid email address. Anyone can create account of anyone and also can access any genuine accounts on that website and place any order at any address.

Verification Of One-Time Passwords - An application on the server system that needs OTP authentication is expected to issue associate degree OTP challenge as delineated on top of.

Given the parameters from this challenge and the secret passphrase, the generator encrypts (or searches) the one-off word that is passed to the server for verification. The server system incorporates, for each user, information including the one-time word from the last notable authentication or the first OTP of the newly initialized sequence.

To authenticate the user, the server decodes the one-time word received from the generator into a 64-bit key. Therefore, pass this key to the secure hash function once. If the result of this operation matches the previous OTP Pending, the authentication is successful and the accepted one-time password is saved for future use.

Attack Possible - There are various attacks possible which includes:

- Spoofing
- Violation of private information

III. SOLUTION

When user enters mobile number it should send OTP to the mobile and the should verify the email address by sending a verification link. Also user should be able to set password to his account and also should be able to login via OTP authentication.

IV. CONCLUSION

There are many authentication methods in practical use today. If they are classified based on usability and security, most of them are classified into security categories that guarantee the security of the user's account using the second factor, but they have appropriate usability I miss it.

The rest is an authentication method that is designed to achieve better usability, but lacks the appropriate security to protect users from communication channel attacks and spoofed server attacks. This study aimed to provide an authentication scheme that fills the gap between security and usability. Another goal was to use smart cards as a second factor to provide security and to use graphical passwords to improve usability.

V. REFERENCES

[1]. A One-Time Password System - N. Haller