IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

Remote Password Authentication and Validation Methods

Shubham Sharma
Dronacharya College of Engineering, Gurgaon

Abstract: *In the old days one used to remember passwords which was the only medium to authenticate and a measure to secure confidential information. With the development in the technology, one can find the vulnerability and can exploit it in the form of hacking and stealing of data, which can result in the loss of company as well as could cause loss of the client. In this project report we will look into various alternatives used in the industry rather than a typical password login system to make the system less prone to hacks and make it more secure and reliable.*

Keywords: Remote password

I. INTRODUCTION

As we see more and more development in technology the data has become more prone to cyber attacks, Thefts which lead to huge loss to the company in terms of money and clients. Due to such scenarios the new methods for authentication were introduced which were used as a medium or a protective layer between the attackers and the data.

In the initial days the data was hacked with the help of the computers itself due to which it was difficult for the system to identify whether it is a user or a machine, to solve this problem captcha was introduced which was difficult for the machines to authenticate which solved the issue. But to secure the data new methods of authentication were required. For more frequent and secure biometric authentication were introduced such as fingerprint sensors which provided more quick authentication to the users.

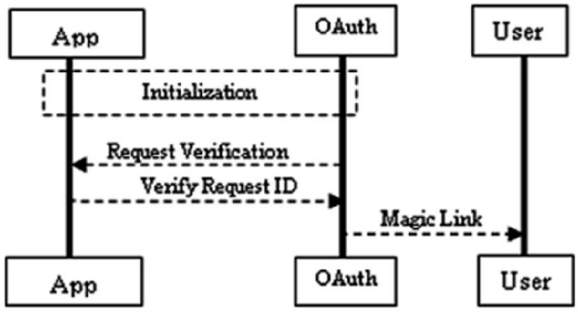
Yet it was not a solution for the big companies for securing the data. The big companies generated different solutions for the issue such as link authentication, which is sent to the registered email id and is valid for a limited period of time. more such methods are defined in the paper below.

II. DIFFERENT METHODS OF PASSWORDLESS AUTHENTICATION

2.1 Link Login Authentication

It is difficult for a person to remember all the passwords he requires, to deal with this problem and provide a secure way to authenticate a login link called “Magic Link” which provides a password-less authentication. It can be a one time code and is valid for a period of time which does not compromise the security.

Figure 1. API Call 1 (for authentication key)



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

Figure 2. API Call 2 (to get authenticated)

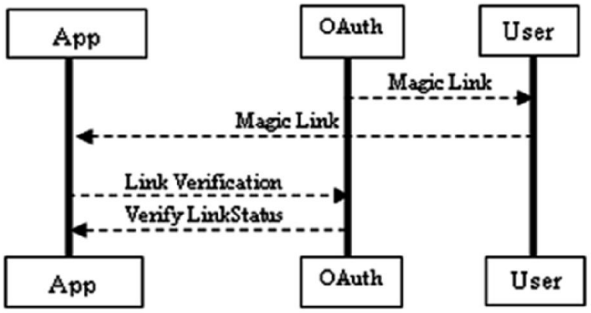


Figure 3. Working: Getting magic authentication link on Email

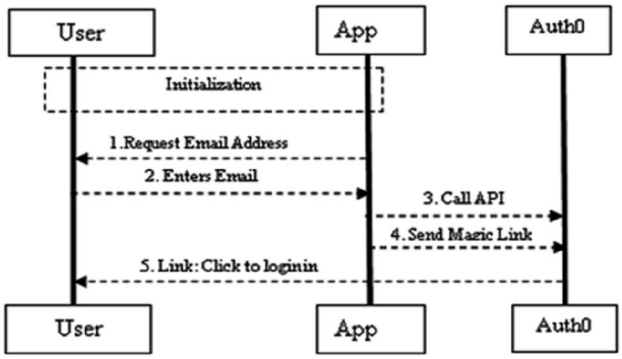
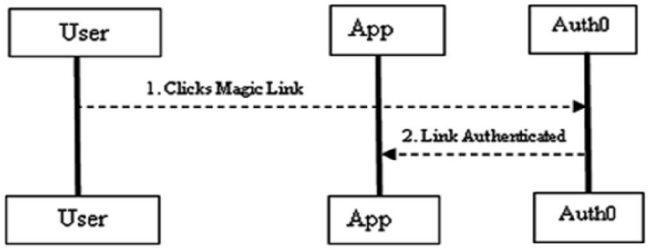


Figure 4. Working: Authenticated login to the user account



2.2 Token Based Authorization

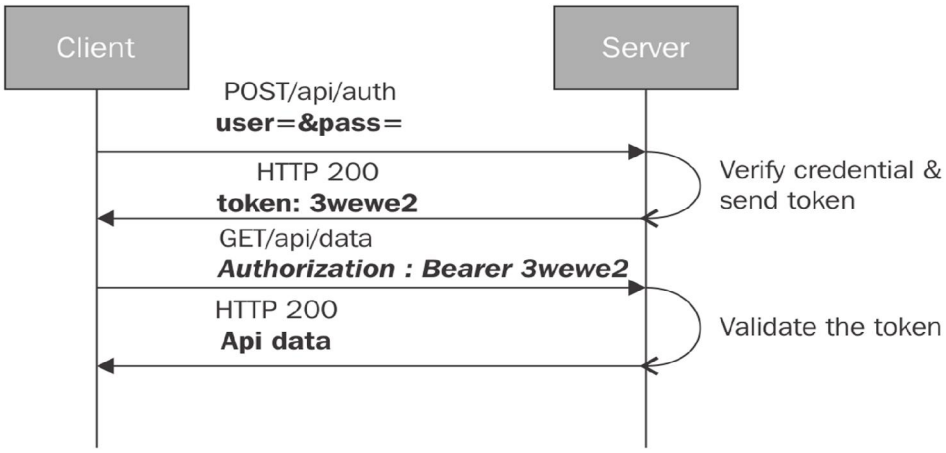
The most common method of token based authorization is OTP. The OTP is a security token which is generated for authentication and is valid only for a short period of time and can only be used once after it expires.

There are various stages for OTP:-

a. **Request-** the user request for the generation of the security token after the user puts the credentials through a server request.
b. **Verification -** the server checks whether the credentials entered are correct or not.
c. **Token submission-** after verification the security token is submitted to the user which is valid for a period of time.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

d. Token verification - when the user tries to use the token it is decoded and verified if the token is encoded and the user is allowed to use the facility.



III. BIOMETRIC AUTHENTICATION

Biometric authentication is an authentication based on the unique traits of the human body which makes it different from one another. Biometric authentication uses these traits to check if the person is the one whom he claims to be. Today we use fingerprint sensors in cell phones all around the world which has become a part of our life.

Another example is the new face detection technology which is used in the newer generation iphone which uses sensors to verify whether the facial features of a person matches for the person or not.