How does the Token-Based Authentication work ?

Last Updated : 13 Mar, 2023

Digital transformation brings security concerns for users to protect their identity from bogus eyes. According to US Norton, on average 8 lakh accounts are being hacked every year. There is a demand for high-security systems and cybersecurity regulations for authentication.

Traditional methods rely on single-level authentication with username and password to grant access to the web resources. Users tend to keep easy passwords or reuse the same password on multiple platforms for their convenience. The fact is, there is always a wrong eye on your web activities to take unfair advantage in the future.

Due to the rising security load, two-factor authentication (2FA) come into the picture and introduced Token-based authentication. This process reduces the reliance on password systems and added a second layer to security. Let's straight jump on to the mechanism.

But first of all, let's meet the main driver of the process: a T-O-K-E-N !!!

What is an Authentication Token?
A Token is a computer-generated code that acts as a digitally encoded signature of a user. They are used to authenticate the identity of a user to access any website or application network.

A token is classified into two types: A Physical token and a Web token. Let's understand them and how they play an important role in security.

- **Physical token**: A Physical token use a tangible device to store the information of a user. Here, the secret key is a physical device that can be used to prove the user's identity. Two elements of physical tokens are hard tokens and soft tokens. Hard tokens use smart cards and USB to grant access to the restricted network like the one used in corporate offices to access the employees. Soft tokens use mobile or computer to send the encrypted code (like OTP) via authorized app or SMS.
- **Web token**: The authentication via web token is a fully digital process. Here, the server and the client interface interact upon the user's request. The client sends the user credentials to the server and the server verifies them, generates the digital signature, and sends it back to the client. Web tokens are popularly known as JSON Web Token (JWT), a standard for creating digitally signed tokens.

A token is a popular word used in today's digital climate. It is based on decentralized cryptography. Some other token-associated terms are Defi tokens, governance tokens, Non Fungible tokens, and security tokens. Tokens are purely based on encryption which is difficult to hack.

What is a Token-based Authentication?

Token-based authentication is a two-step authentication strategy to enhance the security mechanism for users to access a network. The users once register their credentials, receive a unique encrypted token that is valid for a specified session time. During this session, users can directly access the website or application without login requirements. It enhances the user experience by saving time and security by adding a layer to the password system.

A token is stateless as it does not save information about the user in the database. This system is based on cryptography where once the session is complete the token gets destroyed. So, it gets the advantage against hackers to access resources using passwords.

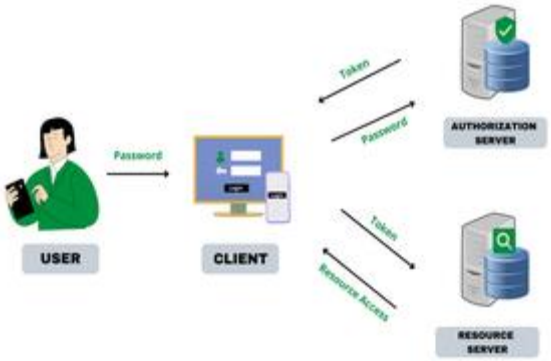
The most friendly example of the token is OTP (One Time password) which is used to verify the identity of the right user to get network entry and is valid for 30-60 seconds. During the session time, the token gets stored in the organization's database and vanishes when the session expired.

Let's understand some important drivers of token-based authentication-

- **User**: A person who intends to access the network carrying his/her username & password.
- **Client-server**: A client is a front-end login interface where the user first interacts to enroll for the restricted resource.
- **Authorization server**: A backend unit handling the task of verifying the credentials, generating tokens, and send to the user.
- **Resource server**: It is the entry point where the user enters the access token. If verified, the network greets users with a welcome note.

How does Token-based Authentication work?

Token-based authentication has become a widely used security mechanism used by internet service providers to offer a quick experience to users while not compromising the security of their data. Let's understand how this mechanism works with 4 steps that are easy to grasp.



How Token-based Authentication works?

1. Request: The user intends to enter the service with login credentials on the application or the website interface. The credentials involve a username, password, smartcard, or biometrics

2. Verification: The login information from the client-server is sent to the authentication server for verification of valid users trying to enter the restricted resource. If the credentials pass the verification the server generates a secret digital key to the user via HTTP in the form of a code. The token is sent in a JWT open standard format which includes-

- **Header**: It specifies the type of token and the signing algorithm.
- **Payload**: It contains information about the user and other data
- **Signature**: It verifies the authenticity of the user and the messages transmitted.

3. Token validation: The user receives the token code and enters it into the resource server to grant access to the network. The access token has a validity of 30-60 seconds and if the user fails to apply it can request the Refresh token from the authentication server. There's a limit on the number of attempts a user can make to get access. This prevents brute force attacks that are based on trial and error methods.

4. Storage: Once the resource server validated the token and grants access to the user, it stores the token in a database for the session time you define. The session time is different for every website or app. For example, Bank applications have the shortest session time of about a few minutes only.

So, here are the steps that clearly explain how token-based authentication works and what are the main drivers driving the whole security process.

Note: Today, with growing innovations the security regulations are going to be strict to ensure that only the right people have access to their resources. So, tokens are occupying more space in the security process due to their ability to tackle the store information in the encrypted form and work on both website and application to maintain and scale the user experience. Hope the article gave you

all the know-how of token-based authentication and how it helps in ensuring the crucial data is being misused.