JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

Token Based Authentication Using IOT

Akshay Hegade[1*], Sindhu K. G[2]

[1]Enterprise Security Division, Symantec Software Solutions Pvt Ltd, Bengaluru, Karnataka, INDIA
[2]Department of Computer Science & Engineering, PDIT, HOSPET, Karnataka, INDIA

DOI: https://doi.org/10.26438/ijcse/v7i2.776779 | Available online at: www.ijcseonline.org

Accepted: 19/Feb/2019, Published: 28/Feb/2019

***Abstract*—** Token Based Authentication is one of the basic mechanism of login that will be required and used in most of the web applications. The token is prima focus in the whole functionality of the product which can not be decrypted by users.

***Keywords*—**Security,Authentication,Authorization.

I. Introduction

Information stored on the websites varies widely in the amount of information available either publicly or privately. On some websites, a full-fledged database of personal information may be available in the form of MDR-Master Data Record.

So security concerns plays a major role in protecting the privacy of the information of the users and company's sensitive data, login functionality is the most basic feature which should be implemented in robust and reliable way, and token based authentication is one of the most widely used type of authentication used by most of the companies.

Authentication based on token is prominent in most of the websites nowadays. Companies using this feature provide an API. And token-based authentication seems to be the most trusted and robust way to handle authentication of the multiple users.

In this approach, sessions and cookies along with any local storage is not used. Instead a token will be used for the purpose of authentication of each user requests.

Description

• When user enters the URL of any of the website, he will be landed on the login in page of the application

• There user will be prompted to fill out the details like Username and Password

• After filling these details, user clicks on login button.

• So it's like from the Client/browser request is sent and its part is completed, the whole of this process can be visualized as one POST request which contains username and password in its request body

• This can be implemented by any of the clients, means it need not be only browser, like CURL or any of the UI Test frameworks like Jasmine, Protractor etc

• Once backend receives the request, which can be implemented in languages like JAVA, C#, Python etc, the user details are fetched are from the request and it is validated against the stored details which can be MDR (Master Data Record) or persisted details coming from the database

• If the user is validated, based on the defined standards a token will be generated and it will be sent in in the response body

• So, now client will have the token information from the received response, and in all the next consecutive request response chain, same token will be sent in the request header
• Here, server will not return something like session or cookie instead it returns the token in the form of JSON/XML in the response body.

II. Related Work

During the early days of the computer evolution there was not much effort put into the security of the computers. Instead much attention was given towards only towards the business part of the computing and mostly related to research works.

Nobody had ever imagined that one day computer will be used so extensively, and that too with the advent of the internet which can pierce to so many corners of the world and into so many fields like from Research to Defense, from Hospitals to Banking [1] and what not.

More the usage of internet more is the threat, with the concept of IOT [2] (Internet of things), where one is more bothered and concerned to do have internet in all of the devices and wants everything to be connected via internet, people are exposed to internet and security vulnerabilities more than ever.!

With these things in mind, many of the security companies like Symantec are coming with many of the different approaches to handle such kind of situations where people are put into grave danger of exposing themselves to the world of internet and there are many prying eyes which are in constant search to find there pray.

Across the world during January 2009, the number of computers which are connected to Internet were estimated at 625,226,456 (625.2 Million), and as of 2016, 40% of the world population is exposed to the world of internet.

So, there are many companies and organizations striving hard to achieve the and address the security issues of the world. Today most of the companies have their products ready but because of the security concerns they are not able to sell to the end users.

Token Based Authentication in Primary Aid

Key points to remember in providing the security:

• Confidentiality is at most concern

• Integrity of the data should be maintained throughout the life cycle of any process

• System should be available with high accuracy

• Authenticity is most important, as with so many websites, people will go for only trusted and authentic websites and companies

• Non-Repudiation should be maintained, nobody can deny the service provided at the later point in time after the request is served

• Encryption and Cryptography is very much important.

III. METHODOLOGY

Existing Authentication Mechanisms:

Different types of Authentication available today are :

1. Server based Authentication[3] :

The server can require a different type of authentication depending on its role and responsibilities. If database is utilized as a server in a typical client/server architecture, certificates are used that are set within a wallet for the database for server-side authentication. However, if server is used to callout to another object or call-back to an object on the client, the server is now acting as a client and so requires its own identifying certificates. That is, in a callout or call-back scenario, the server cannot use wallet generated for database server-side authentication

2.SAML Authentication[4]:

Security Assertion Markup Language is a XML based open standard data format for defining and exchanging authentication along with authorization of data/content between the two parties. It is product of company called OASIS Security Services Technical Committee. SAML is initiated on 2001, and from then there are many updates done and current version is called SAML 2.0

SAML, provides SSO from the web browser perspective unlike any of the existing Open LDAP Implementation like that of Pulse secure of CISCO or any other.

3.OAUTH[5] :

Authentication OAuth is an open standard of authentication and authorization which is commonly used by some of the tech giants for some of their applications.

Companies which use OAuth are :

• Microsoft, Google, Twitter, One Network etc

Since OAuth provides secured delegate access to serve the resources of the host on behalf the owner of the resource it is used to generally give limited access for the vendor applications. It is integrated seamlessly with HTTP Protocol making it more popular than SAML.

IV. PROPOSED SYSTEM

Token based authentication is highly used on the different websites[6] nowadays. With most of the web companies using an API based service provider approach, tokens are the best suited to handle authentication for the multiple users who will be using the system.

The main reasons for choosing token based authentication for any of the websites are:

• It is Stateless and can scalable to any number of server

• It makes application to be ready for Mobile application

• Third party applications can use host authentication

• It Provides much needed extra security

➢ Who Uses Authentication based on Token ?

• Google, Facebook, Twitter, Github, etc

➢ Why Tokens Came Around ? Before understanding the importance of token based authentication, it is necessary to understand how authentication has been done in the past for the various applications. From the study it is found that no other authentication mechanisms which are discussed in earlier sections are as effective as token based authentication.

➢ How Authentication based on Token works ? It is stateless. No user related information including name, email etc are stared in any state of the sessions.

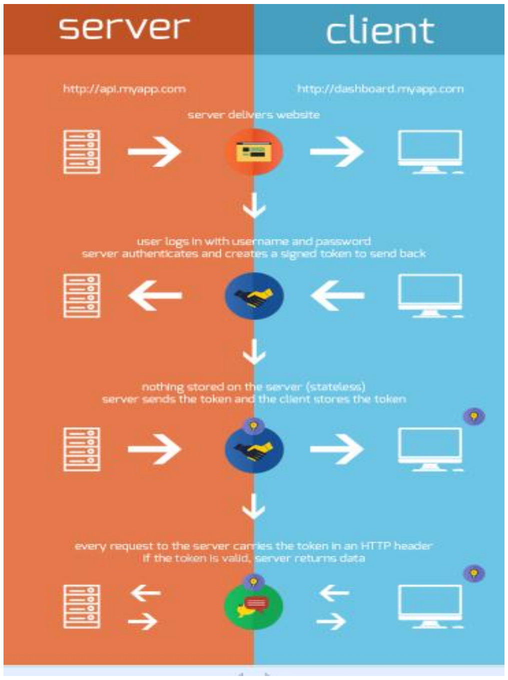
This concept alone addresses many of the existing issues/concerns of storing many of the sensitive information on the server

Since there exists literally no session information about the user session, which means application can scale and add any number of extra servers during runtime dynamically here the concept of elastic servers will come into the picture.
In short this is how it works :
• User who is trying to login requests for Access by providing valid credentials (Username and Password)
• Application/Backend engine validates the correctness of these credentials
• A signed token will be issued by Backend engine on successful validation
• Client such as browser/CURL/JASMINE/Protractor stores this information forwards the token with next consecutive requests
• Application/Backend engine serves these requests after validating token
Once information is authenticated, token is generated and any further processing of the request can be done based on the generated token. Even permission based tokens can be generated along a third party applications like mobile app, and they can access the data of the application, but it will be restricted information which will be in the hands of host application.

The benefit of Token Based Authentication :
• Stateless and Scalable systems
• Provides High Security
• Supports Multiple domains and platforms
• API Rich makes it more extensible
• Provide great deal of Standard based approach

When creating the token, there will be few options, like how tokens should be generated, based on what criteria tokens should be formed is decided. This can include some standard details like date and time component along with time zone and users ip details from which he has logged in. By using all this information one standard token can be generated.

By having standard based token, this will come in handy during the time of debugging of the any kind of information during any of the failure of the systems, as based on the generated token many of the information can be found like user’s IP address, time zone and exact date and time of login etc.


server
client
http://api.myapp.com
http://dashboard.myapp.com
server delivers website
user logs in with username and password
server authenticates and creates a signed token to send back
nothing stored on the server (stateless)
server sends the token and the client stores the token
every request to the server carries the token in an HTTP header
if the token is valid, server returns data

Fig[1] : Infographic representation of the token based authentication process

IV. RESULTS AND DISCUSSION

• Token-based authentication is predominantly used on the websites and apps since it allows users
to stay logged onto a websites and apps without the use of cookies.
• In addition to a more user-friendly experience, tokens are more secure than cookies because
they can be used to replace a user’s actual credentials. By this way user credentials are masked
from the outside world
• Cookies and tokens have the similar purpose, but tokens don’t need to be stored in the server
unlike cookies in order to work. With tokens, the server only needs to verify that the token is alive, which is determined by the TTL(Time to Live) before authorizing any request.

V. CONCLUSION AND FUTURE SCOPE

• Token based authentication is best suited for all the new age websites where user authentication is required. Because of robustness in nature it provides, an edge over all the existing technologies.

• Even in IOT platforms, usage of token based authentication are being thought of [7]
• In the informative websites also(which does not have authentication mechanism), we should use token based authentication along with https, and these token should be

formed based on the user's ip and geo-location. And till the token is valid we can cache the data onto the device which will enhance the user experience.

REFERENCES

[1] Mrunal A. Mahajan, "*An approach for securing SWIPING MACHINE transactions*" IJSRCSE, Vol.06 , Special Issue.01 , pp.68-72, Jan-2018

[2] Priyang Bhatt, Bhasker Thaker, Neel Shah, "*A Survey on Developing Secure IoT Products*", Isroset-Journal Vol.6 , Issue.5 , pp.41-44, Oct-2018

[3] Jim Stabile, Robert Pang, Mala Anand Oracle Corporation, "An Authentication Model for a Web Application Server" Sixth International World Wide Web Conference : POS749

[4] OASIS Security Services TC, "*Security Assertion Markup Language (SAML) V2.0 Technical Overview*" sstc-saml-tech-overview-2.0

[5] Ramanpreet Singh Lamba, "*OAUTH – "A NEW ERA IN IDENTITY MANAGEMENT" AND ITS APPLICATIONS*" White Paper, External Document, Infosys Limited

[6] Muhamad Haekal, Eliyani, "*Token-based authentication using JSON Web Token on SIKASIR RESTful Web Service*" *ISBN: 978-1-5090-1648-8*

[7] Timothy Claeys, Franck Rousseau, Bernard Tourancheau "*Securing Complex IoT Platforms with Token Based Access Control and Authenticated Key Establishment*" hal-01596135

Authors Profile

Mr. Akshay Hegade pursed Bachelor of Engineering from SDM, Visvesvaraya Technological University,Belgaum in the year 2010, and Master of Technology from SDM, Visvesvaraya Technological University, Belgaum in the year 2016. He is member of syllabus forming committe KLEIT Hubli 2012 to 2015. He is currently working as Senior Software Engineer, Enterprise Security Division, Symantec Software Solutions Pvt Ltd, Bengaluru. He has 8 years of experience in the field of software development.

Ms. Sindhu K.G pursed Bachelor of Engineering from PDIT, Visvesvaraya Technological University,Belgaum in the year 2012, and Master of Technology from SDM, Visvesvaraya Technological University, Belgaum in the year 2016. Currently working as Assistant Professor in Department of Computational Sciences & Engineering. She has published 2 journal papers in reputed international journals. She has 5 years of teaching experience and 1 years of Industry Experience