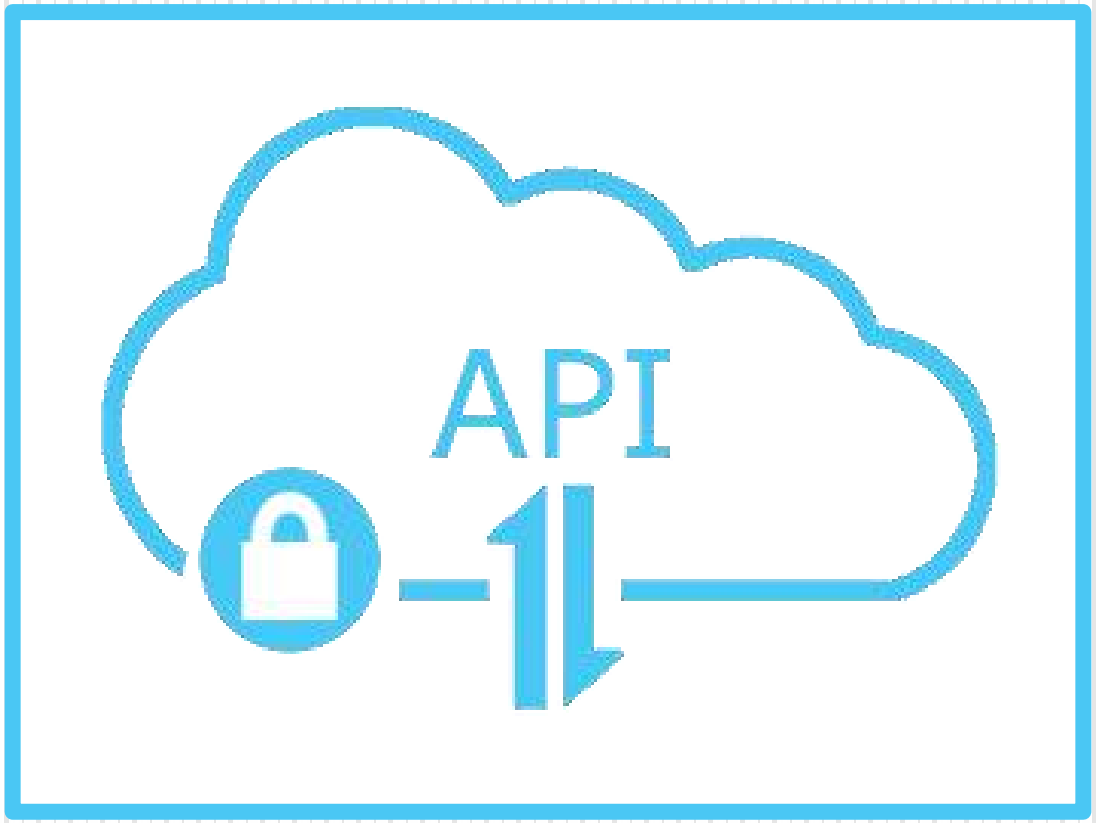
Virtuoso Infotech Pvt. Ltd.

About Virtuoso Infotech

- Fastest growing IT firm; Offers the flexibility of a small firm and robustness of over 30 years experience collectively within the leadership team.
- Technology expertise & passionate team.
- Successful client engagements across India, USA, UK, Australia and Argentina.
- Handle enterprise solutions that involve **30,000 active users**, more than 20 servers, **data volume as big as 5 million entries per day.**

API [Network Communication] Security



- Bhargav Mehta

Agenda

- Introduction to Web API and Security
- Importance
- Major types of Attacks
- Demo
- Avoiding the attacks and Securing the API

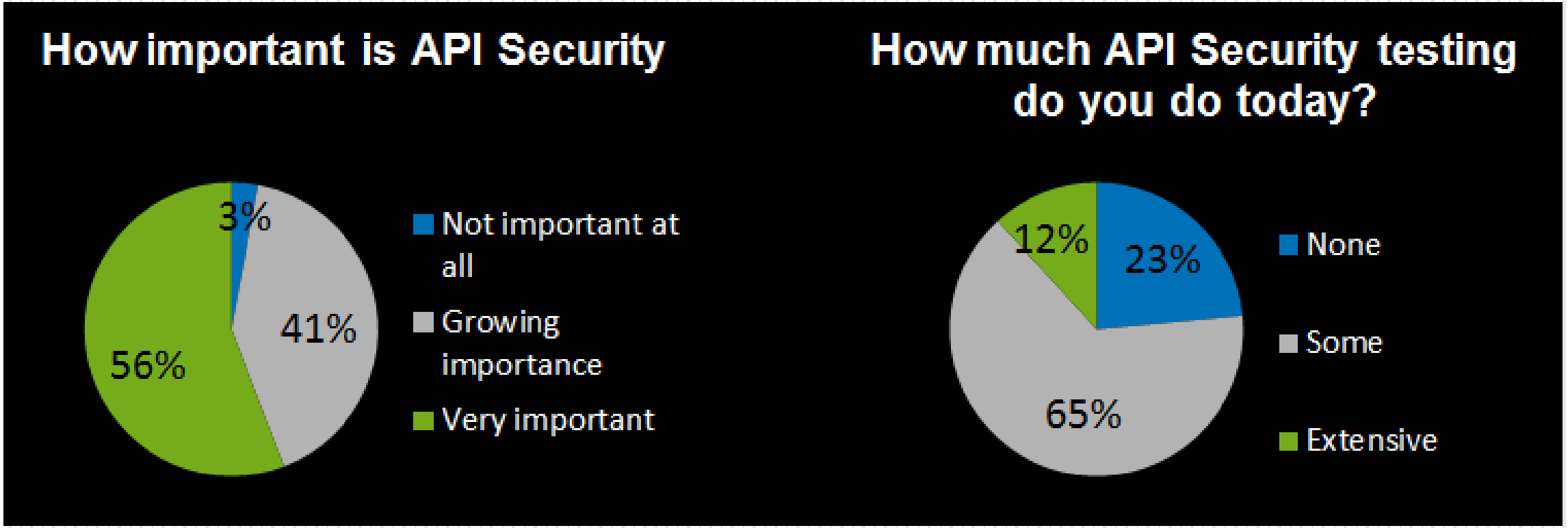
Introduction

- What is a network ?
- What is cloud computing?
- What are different modes of communication between server and an endpoint.
- What is a web API?
- Security.

Introduction to Web API and Security

- APIs are a critical aspect of business delivery in the digital world – they connect mobile applications, the Internet of Things, and providing the fabric that links internal business processes.
- So we would not want hackers to use an API to access the information housed in your mobile app, devices in your home, or processes that could cripple the entire system and business if they were compromised.
- Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a network and network-accessible resources.

Importance of Web API Security



- Smartbear and Axway

API Security Breaches

- Facebook – Over 80 million user's data exposed between 2013 and 2015 through APIs. This was used for political planning in US elections.
- Snapchat – Users could locate unknown phone contacts, add them to their friend's list and communicate with them from within the application.
- IRS – An exposed tax transcript API led the hackers to steal 1,00,000 citizen's tax returns.
- There are a lot more ….

Major types of Attacks - Man in middle

- Attacker intercepts the connection between the endpoints and relays messages between them.
- Endpoints believe they are communicating directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.
- Used to steal personal information, login credentials, account details or credit card numbers.
- Hacker can modify requests to get the additional data not intended for that user; And also modify the responses so that the endpoint functions opposing the system and in a way that benefits hacker.

Major types of Attacks – DoS / DDoS

- This is a cyber-attack in which the perpetrator seeks to make a network resource unavailable by flooding the services with superfluous requests in an attempt to overload systems and prevent legitimate requests.
- In a distributed denial-of-service attack, the incoming originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.
- On March 1, 2018, GitHub was hit by an attack of 1.35 terabits per second
- This can be stopped by using rate-limiting.

Major types of Attacks - Injections

- This type of attack allows an attacker to inject code into a program or query or inject malware onto a computer in order to execute remote commands that can read or modify a database, or change data on a server.

- SQL Injection, Format String Attack, Buffer Overflow, XPath Injection, Cross-site Scripting (XSS)

Avoiding the attacks and Securing the API

- SSL is absolutely must.

- Sensitive information as parameters in HTTP requests – Big NO ..!!!

Security - Basics

- Do Not Mix TLS and Non-TLS Content
  - This includes content from unrelated third party sites.
- User or resource ID should be avoided. Use UUID instead.
  - Use /me/orders instead of /user/654321/orders.
- Don't return sensitive data like credentials, Passwords, or security tokens.
- Consider Adding Timestamp header in Request-Response
  - The server will compare the current and request timestamp. Only accept if it is within a reasonable timeframe.
  - Encrypt it for more security.
- Validate user input,
  - Avoid common injection vulnerabilities.

Security - Headers

- Use "Secure" Cookie Flag for all user cookies.
  - Failure to use the "secure" flag enables an attacker to access the session cookie by tricking the user's browser into submitting a request to an unencrypted page on the site.
- Prevent Caching of Sensitive Data
  - One option is to add anti-caching headers to relevant HTTP responses, ["Cache-Control: no-cache, no-store" and "Expires: 0“]. The response should also include the header "Pragma: no-cache“
- Send Content-Security-Policy: default-src 'none' header.
  - An added layer of security that helps to detect and mitigate Cross Site Scripting (XSS) and data injection attacks

Security - Headers

- Send X-Content-Type-Options: nosniff header.
  - This prevents client from “sniffing” the asset to determine if file type is different than what is declared by the server.
- Send X-Frame-Options: deny / SAMEORIGIN header.
  - Forbids a page from being displayed in a frame
- Remove fingerprinting headers - X-Powered-By, Server, X-AspNet-Version, etc.
- Force content-type for your response, if you return json then your response content-type should be application/json.
- Return the proper status code according to the operation completed. (200 OK, 400 Bad Request, 401 Unauthorized)

Security – Extra step goes a long way

- HTTP Strict Transport Security (also named HSTS)
  - Strict-Transport-Security: max-age=31536000; includeSubDomains
- SSL Certificate / Private Key Pinning
  - A host or service's certificate / public key can be added to an application during development, or it can be added upon first encountering the certificate or public key.
  - Pinning is the process of associating a host with their expected X509 certificate or public key. In this case, the advertised identity must match the value pinned.
- When inserting values into the browser DOM, consider using .value/.innerText/.textContent rather than .innerHTML updates
  - This protects against simple DOM XSS attacks.
- Access Control - Quotas & Throttling

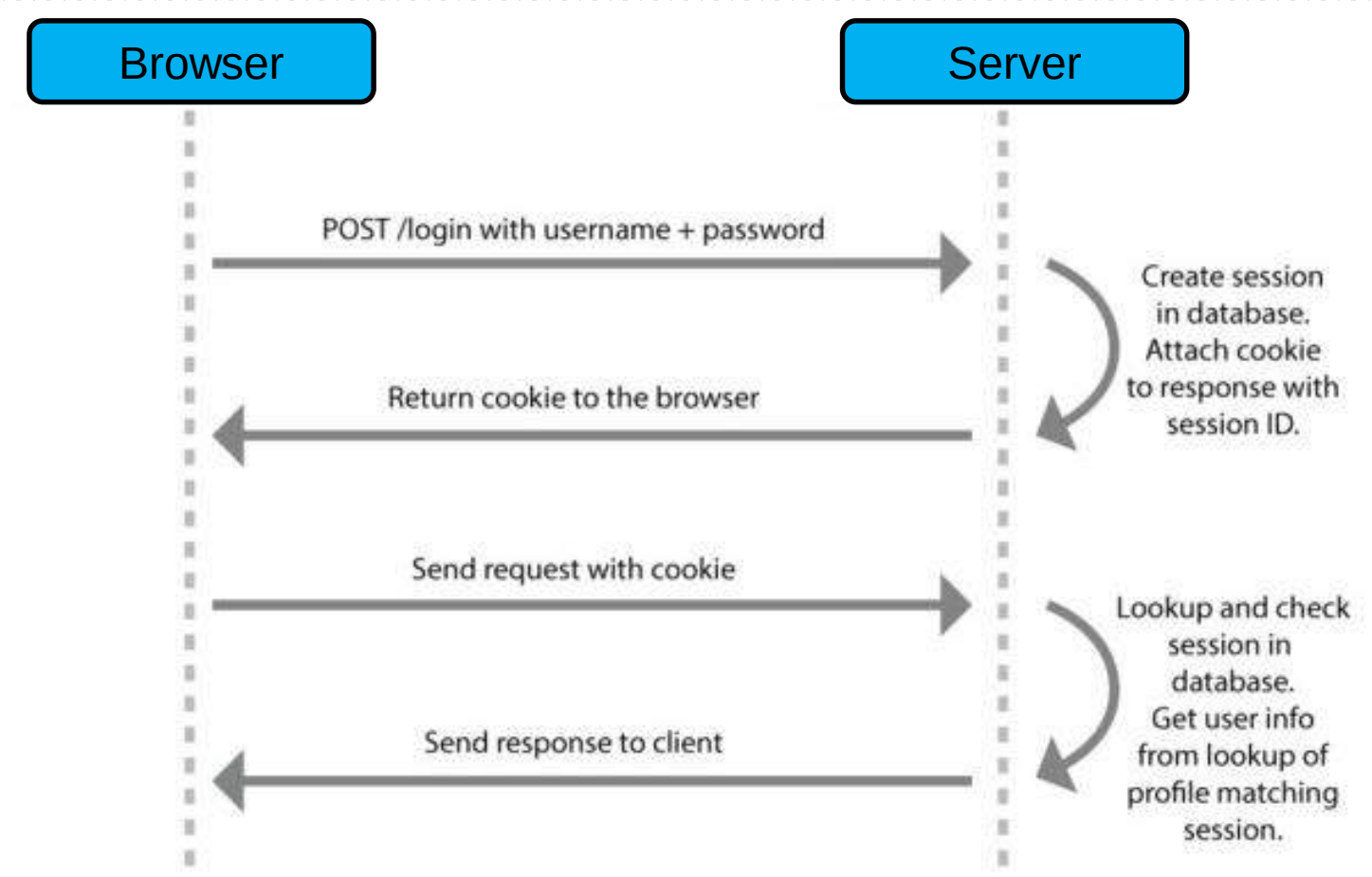
Deep Dive – Authentication & Authorization

- HTTP Basic Authentication - Don't use this
  - Authorization: Basic base64(username:password)

- Digest Schemes
  - Most secure but too difficult and mostly overkill for most applications.
  - password has been hashed by a server provided nonce

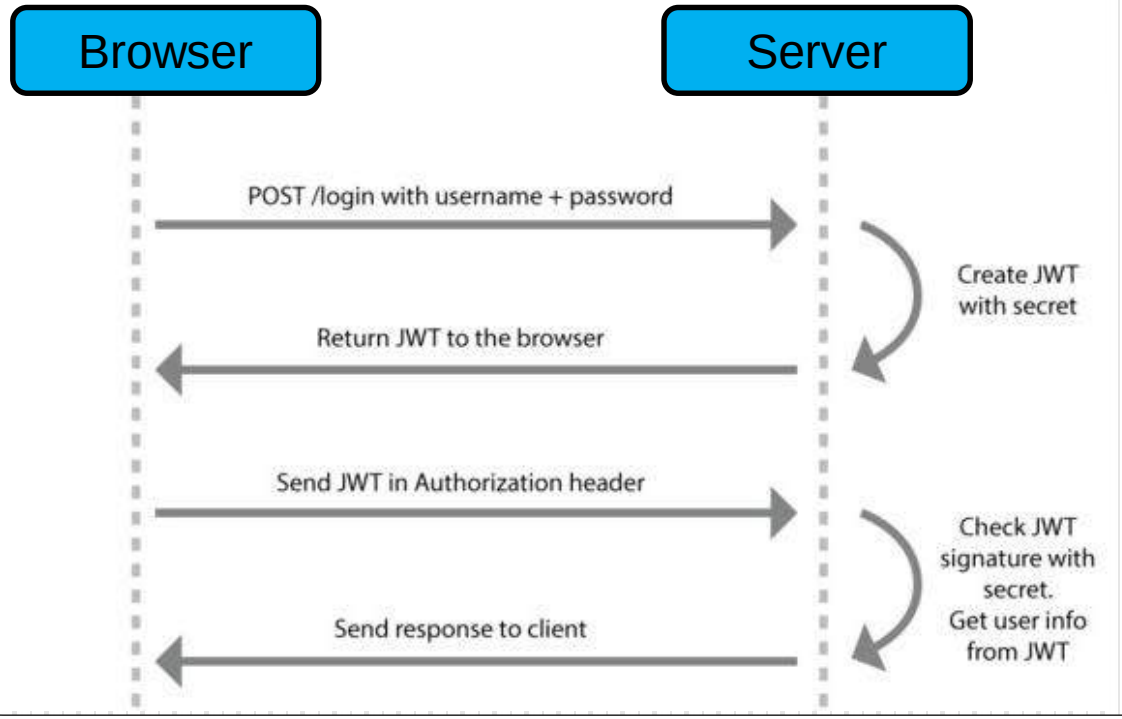
Deep Dive – Authentication & Authorization

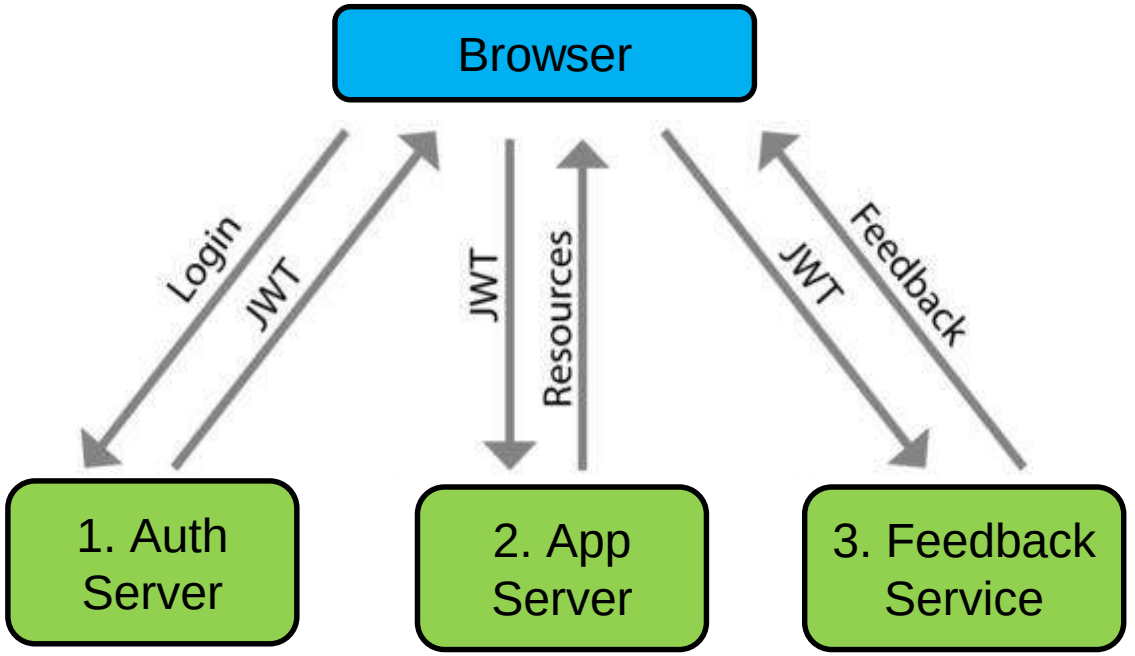
- Session Cookies



Deep Dive – Authentication & Authorization

- JSON Web Tokens [JWT]
  - Open standard for creating tokens that assert some number of claims.
  - Replacement for session cookies as nowadays we have applications contacting multiple backends. In these types of scenarios, the session cookie we get from one server won't correspond to another server.





Deep Dive – Authentication & Authorization

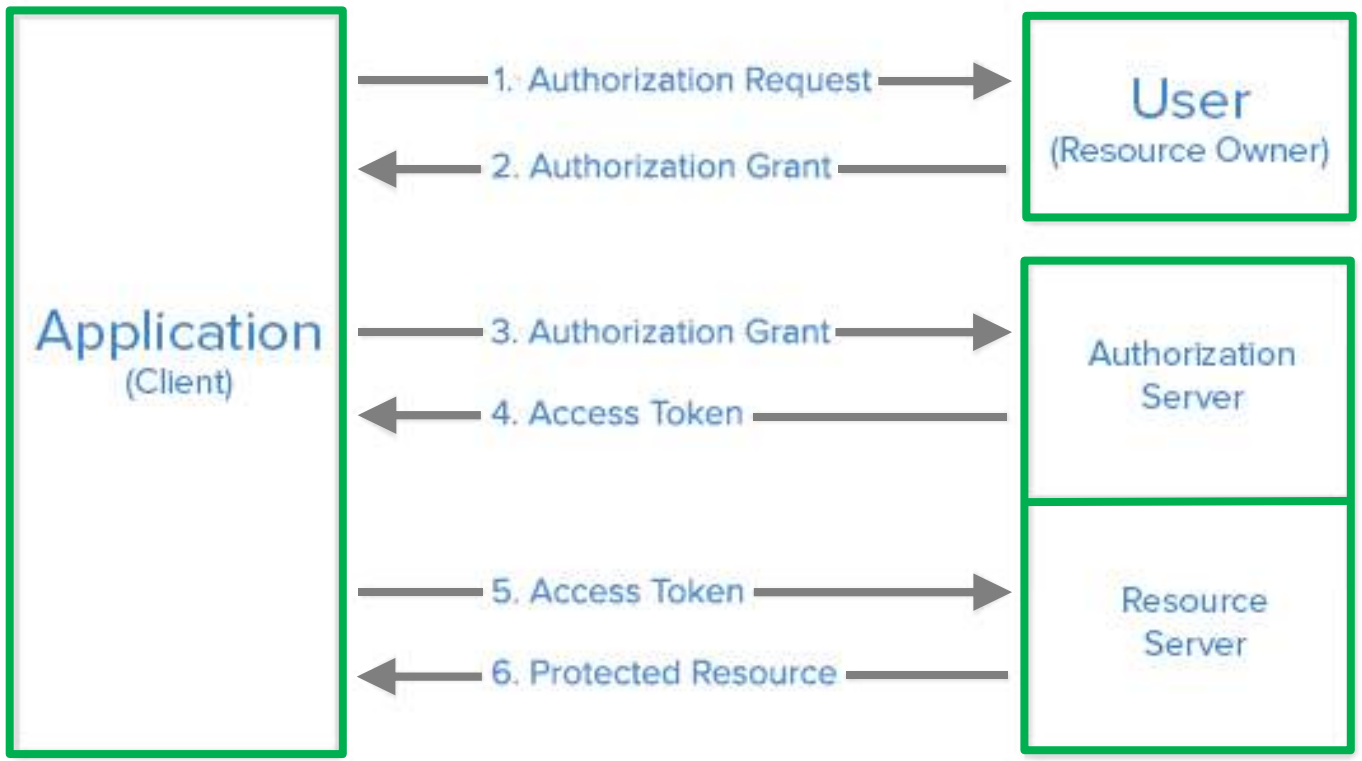
Header	{ **"alg"** : "HS256", **"typ"** : "JWT" }	Identifies which algorithm is used to generate the signature.
Payload	{ **"loggedInAs"** : "admin", **"iat"** : 1422779638 }	Contains a set of claims
Signature	HMAC-SHA256(base64urlEncoding(header) + '.' + base64urlEncoding(payload), secret)	Securely validates the token.

const token = base64urlEncoding(header) + '.' + base64urlEncoding(payload) + '.' + base64urlEncoding(signature)

Authorization: Bearer eyJhbGci.....yu5CSpyHI

Deep Dive – Authentication & Authorization

- OAuth 2.0
  - Generally used for giving 3rd party access to the APIs.
  - OAuth provides to clients a "secure delegated access" to server resources on behalf of a resource owner



Security – Last but not the least

- Code Review
- Audit logs
- Ensure that all components of your services are statically scanned by Antivirus software before pushing to production.
  - Including vendor libraries and other dependencies.
- Vulnerability And Penetration Testing

'Security is a not a product, but a process.' It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.

-- Bruce Schneier

Thank You!

Virtuoso InfoTech Pvt. Ltd.
4th Floor, Victory Landmark, Opp. D-Mart,
Behind Dominos Pizza, Baner, Pune.

+91 8087081318
support@virtuosoitech.com

www.virtuosoitech.com