UVA CNS Spring
2019

Do's and Don'ts of API Security

By Samuel Spelsberg

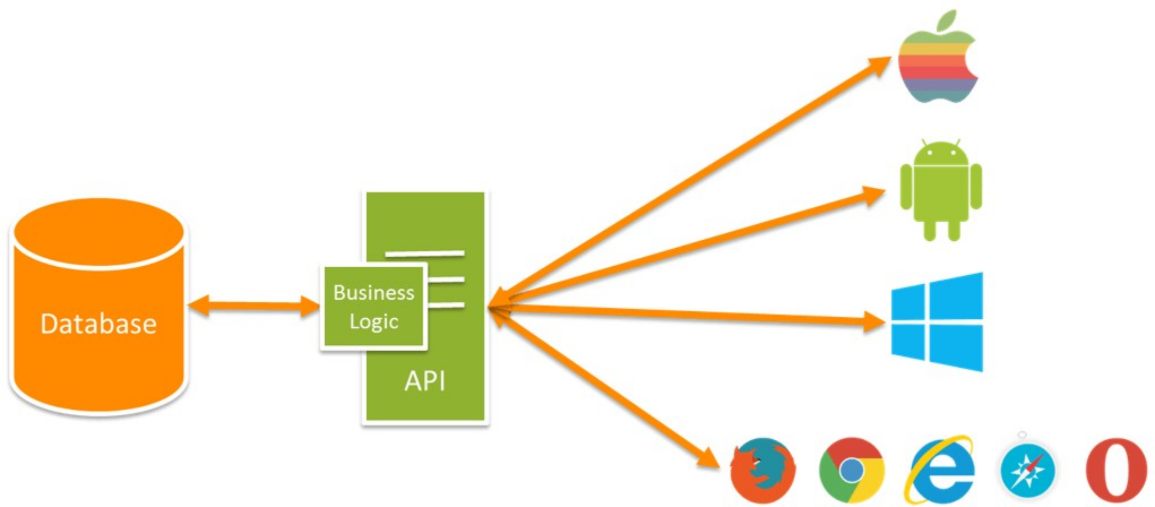
What Does API Mean?

{ api }

Application Programming Interface

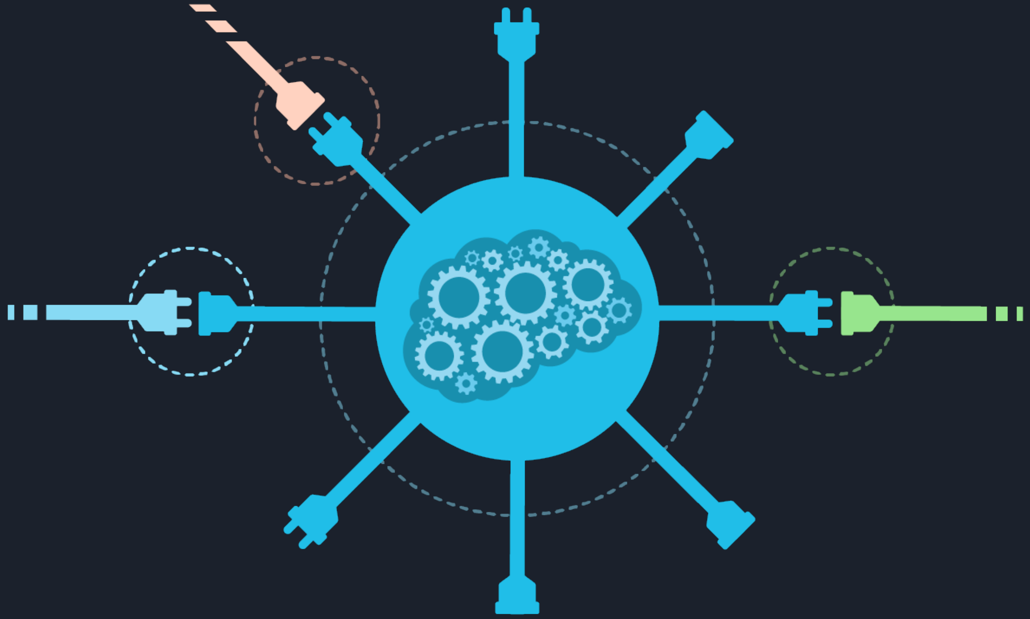
From Google:

"a set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service".

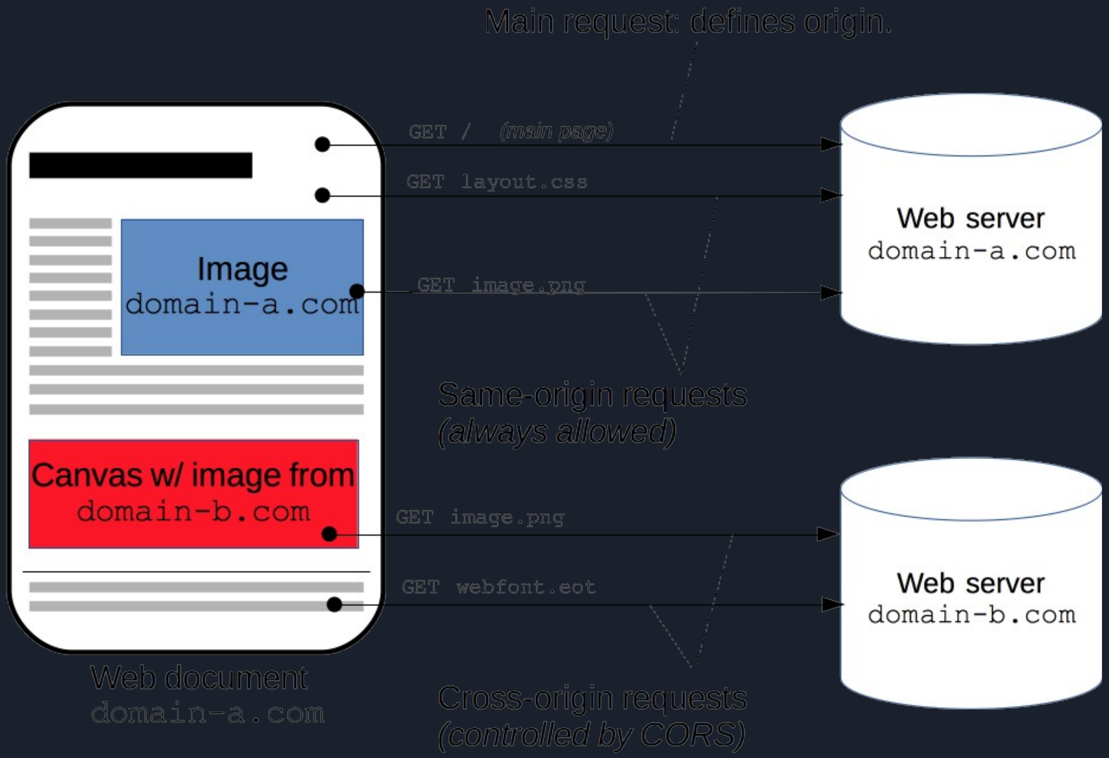


What is API Security and Why is it Important?

Due to the open facing nature of APIs and their access to features or data of a service, they must be taken care of and built with caution.



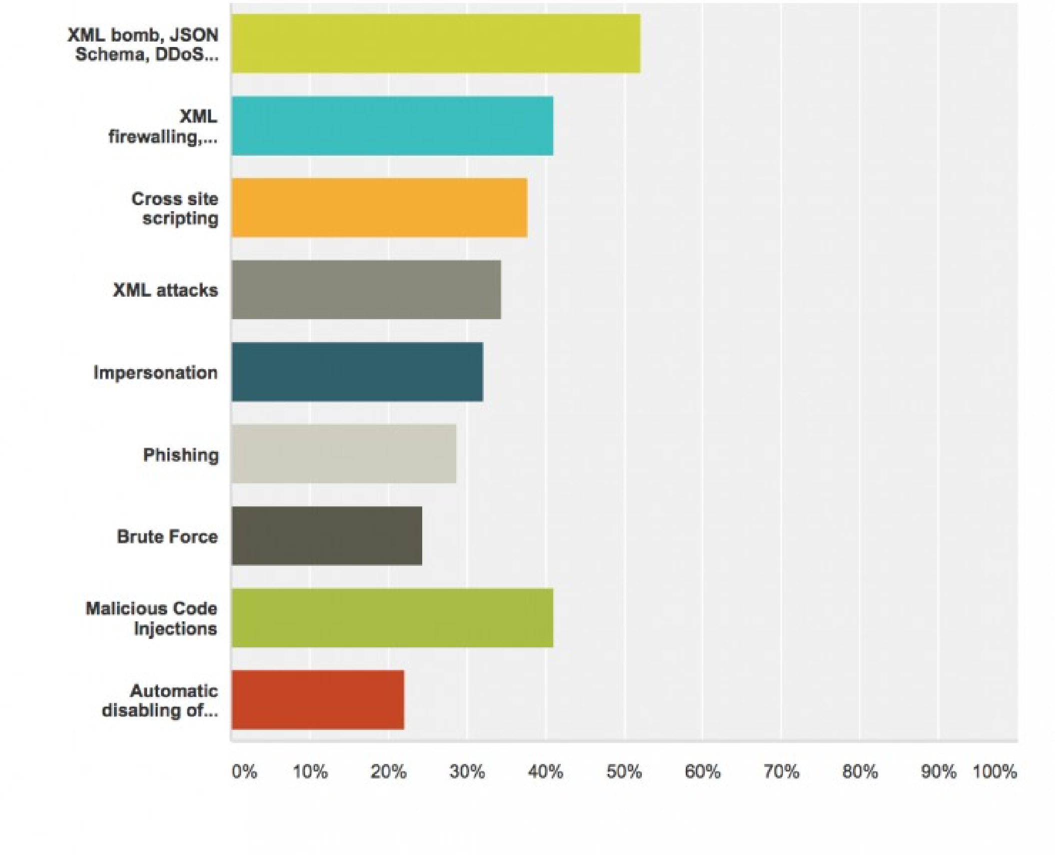
Using An API


Main request: defines origin.
GET / (main page)
GET layout.css
Image
domain-a.com
GET image.png
Web server
domain-a.com
Same-origin requests
(always allowed)
Canvas w/ image from
domain-b.com
GET image.png
GET webfont.eot
Web server
domain-b.com
Web document
domain-a.com
Cross-origin requests
(controlled by CORS)

Examples of Useful APIs

Five Common Weaknesses

Common Attacks

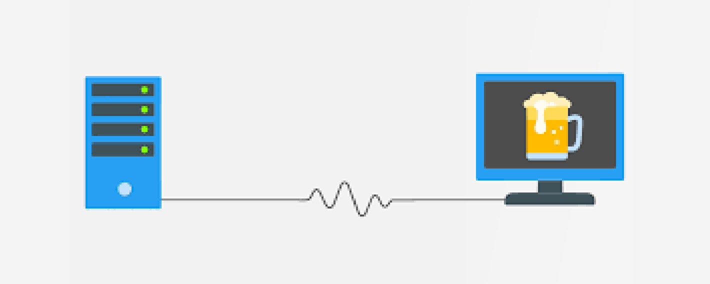


Survey of 200 System Architects in Large Tech Companies

https://blog.akana.com/iryanb-top-five-api-weaknesses/

1/5 - Session Hijacking / Identity Theft

- ❑ Intercepting:
  - ❑ Man/Bot in the Middle
  - ❑ Packet Capture
  - ❑ Replay Captured Data



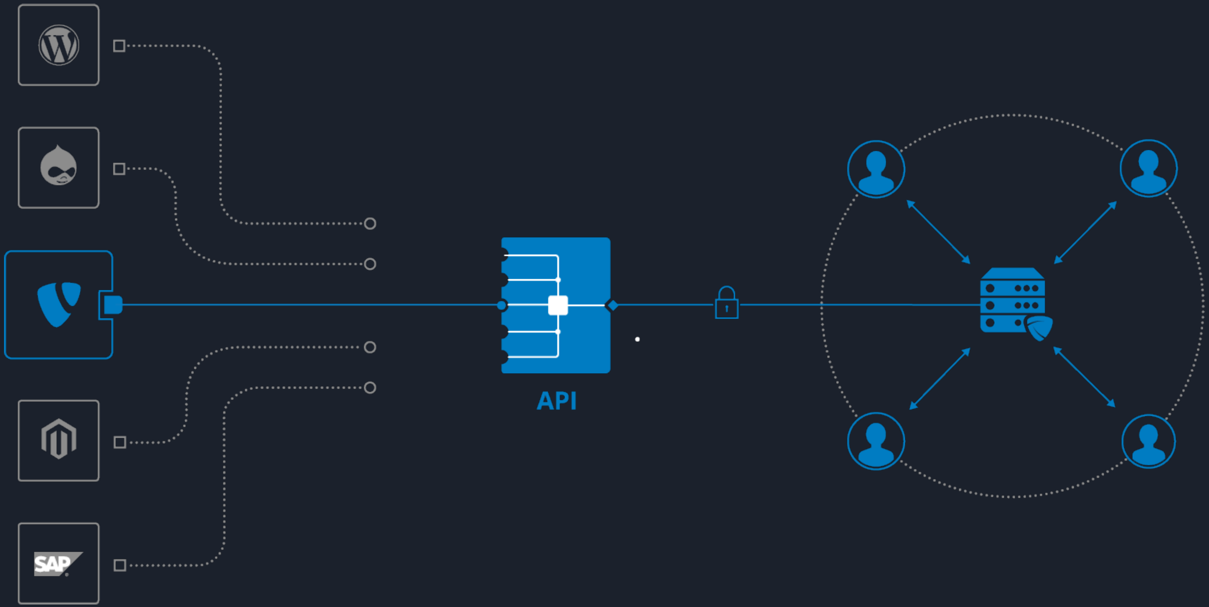
- ❑ Brute Force:
  - ❑ "Replay Attacks"
- ❑ Phishing:
  - ❑ Stealing credentials

2/5 - SSL Protocol Downgrade

- ❑ Outdated Methods
- ❑ Weak Protocols
- ❑ Missing Zero Day Patches

3/5 - Authenticated but not Authorized API Clients

- ❑ User verifies normally
- ❑ Attempts to reconstruct API requests in attempt to access unauthorized services or information



4/5 - Rooted Mobile Devices leaking client application IDs and shared secrets

- ❑ Cleartext information written in code
- ❑ Encryption only at the protocol level

5/5 - Malicious Code / SQL Injections

- Valid users with malicious intent
- Data leaks

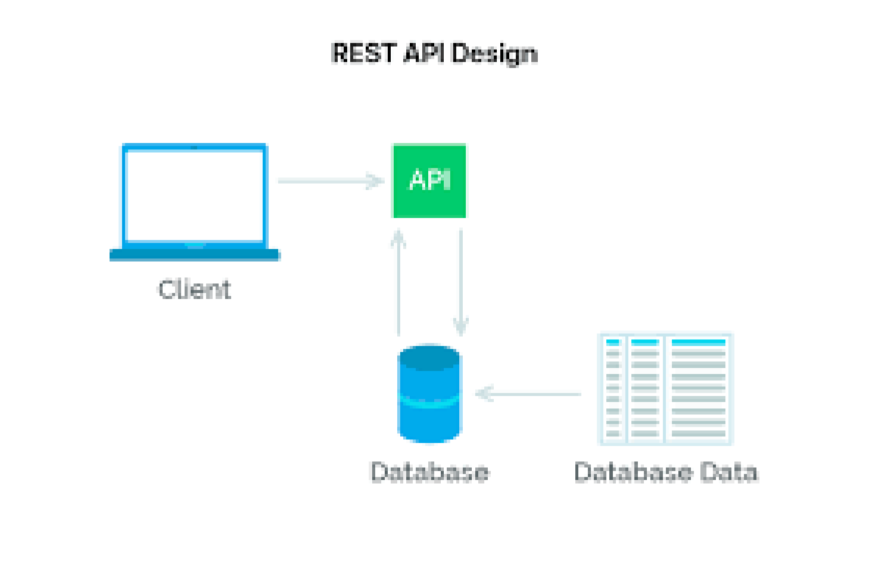
DO's

First, What is RESTful API?

Representational State Transfer

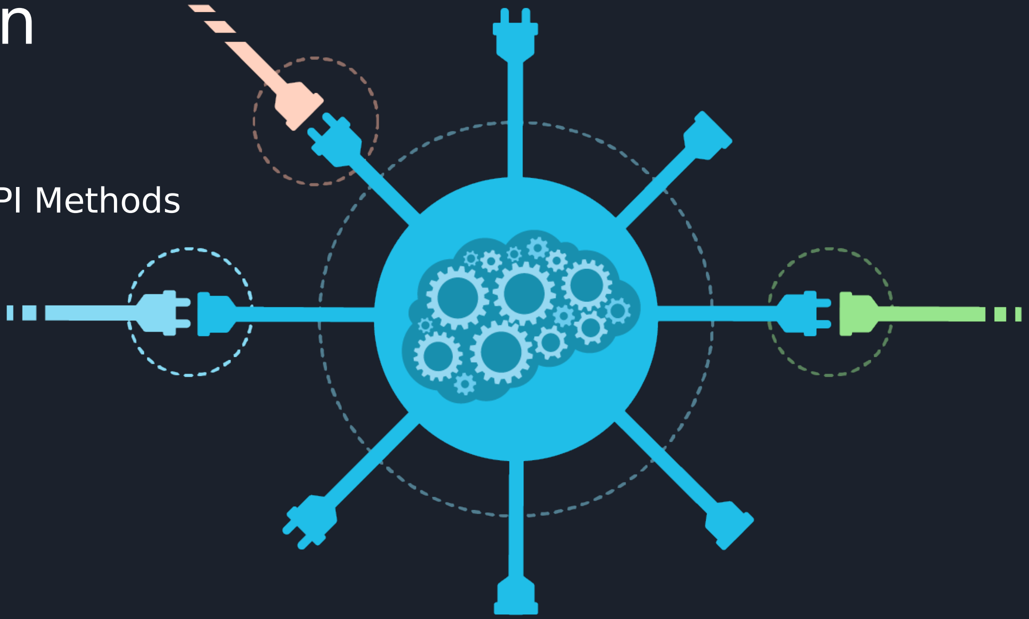
A RESTful API is an application program interface (API) that uses HTTP requests to GET, PUT, POST and DELETE data.

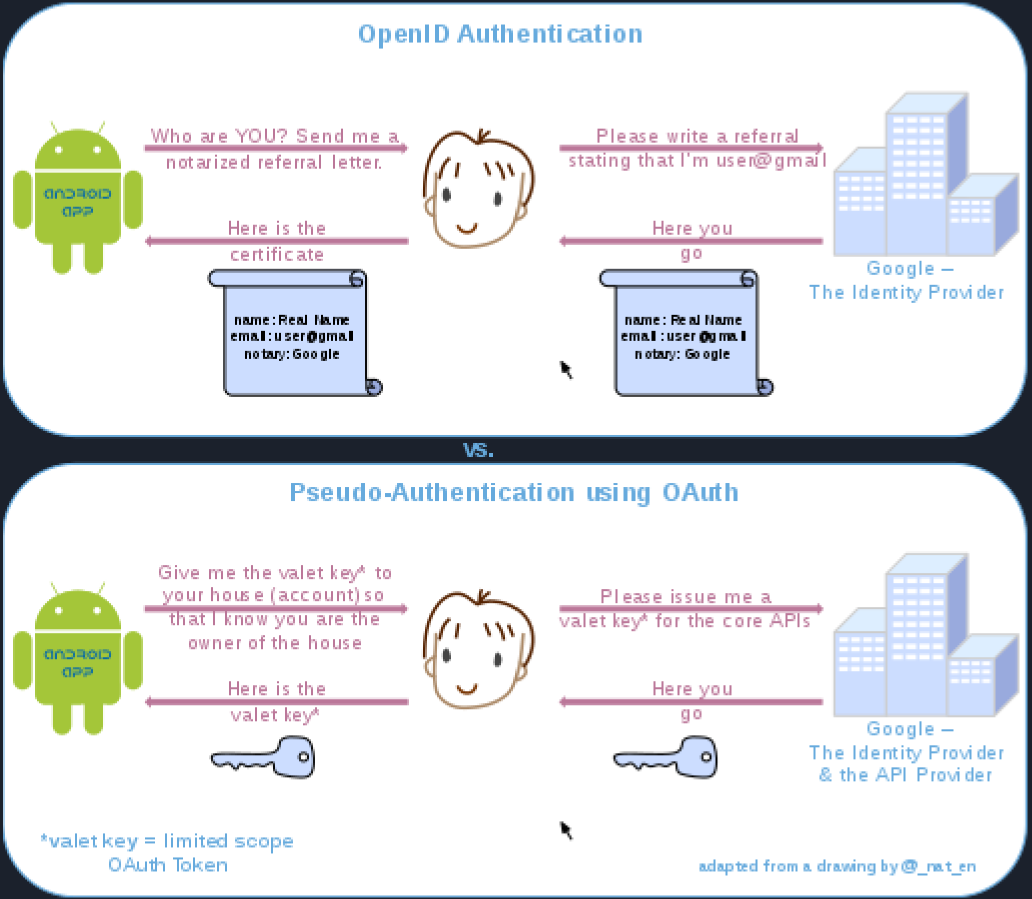
Most common form of API



1/5 - Authorization

- ❑ Protect Access to HTTP and API Methods
- ❑ OAuth
- ❑ Protect from CSRF Attacks





OpenID Authentication

Who are YOU? Send me a notarized referral letter.

Please write a referral stating that I'm user@gmail

Here you go

Here is the certificate

vs.

Pseudo-Authentication using OAuth

Give me the valet key* to your house (account) so that I know you are the owner of the house

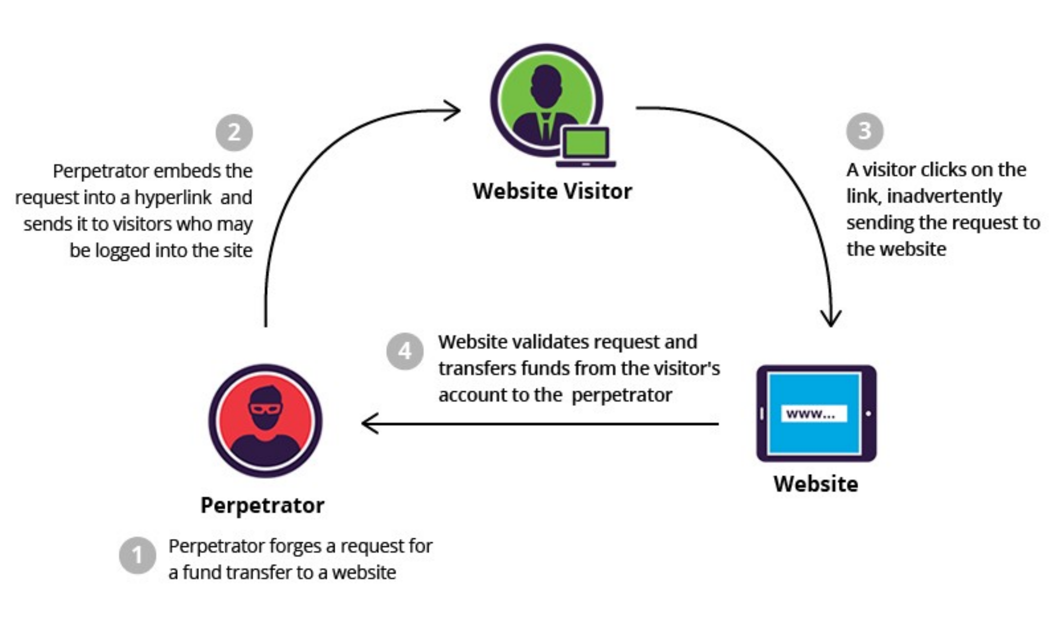
Please issue me a valet key* for the core APIs

Here you go

Here is the valet key*

*valet key = limited scope OAuth Token

adapted from a drawing by @_nat_en



Website Visitor

Website

Perpetrator

1 Perpetrator forges a request for a fund transfer to a website

2 Perpetrator embeds the request into a hyperlink and sends it to visitors who may be logged into the site

3 A visitor clicks on the link, inadvertently sending the request to the website

4 Website validates request and transfers funds from the visitor's account to the perpetrator

2/5 - Input Validation

- ❑ Assist the user
  Assist the user > Reject input > Sanitize (filtering) > No input validation
- ❑ URL Validation
- ❑ Validate Content Types

Common names for common input tampering attacks: forced browsing, command insertion, cross site scripting, buffer overflows, format string attacks, SQL injection, cookie poisoning, and hidden field manipulation.

3/5 - Output Encoding

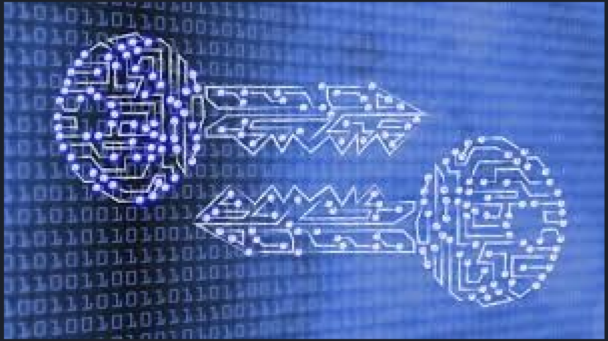
- ❑ Security Headers
- ❑ JSON Encoding

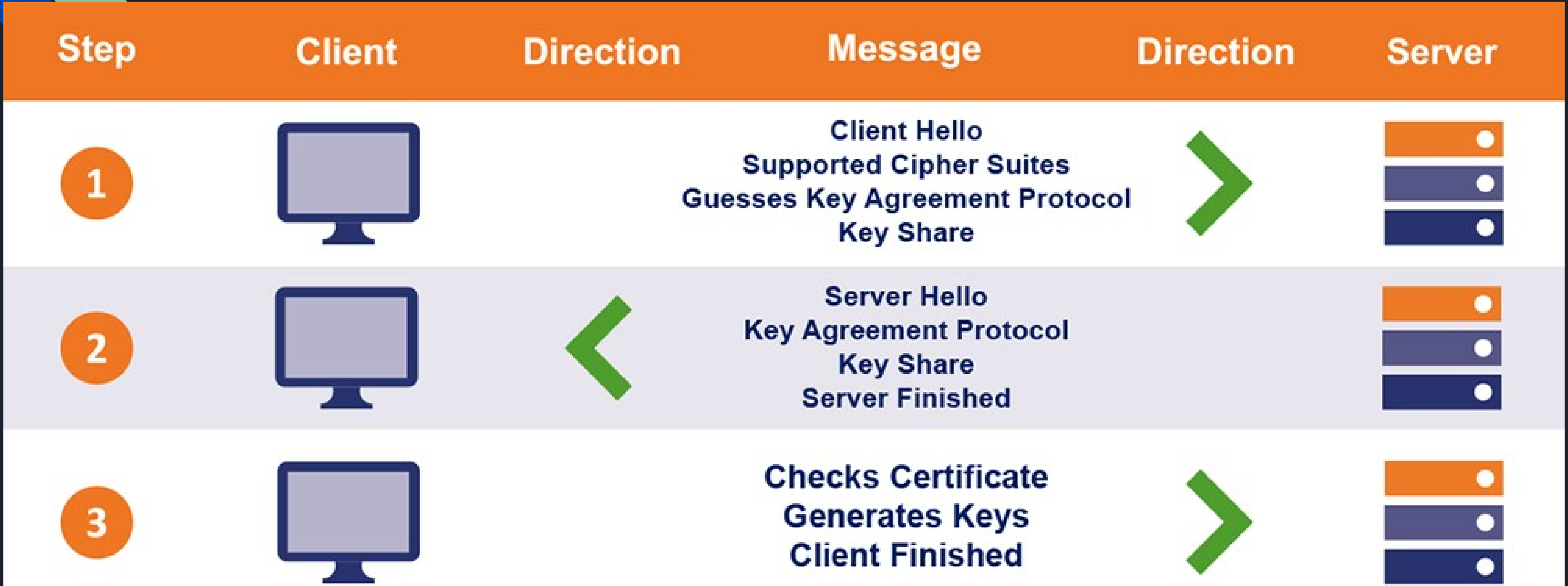
4/5 - Cryptography

❑ TLS - Transport Layer Security

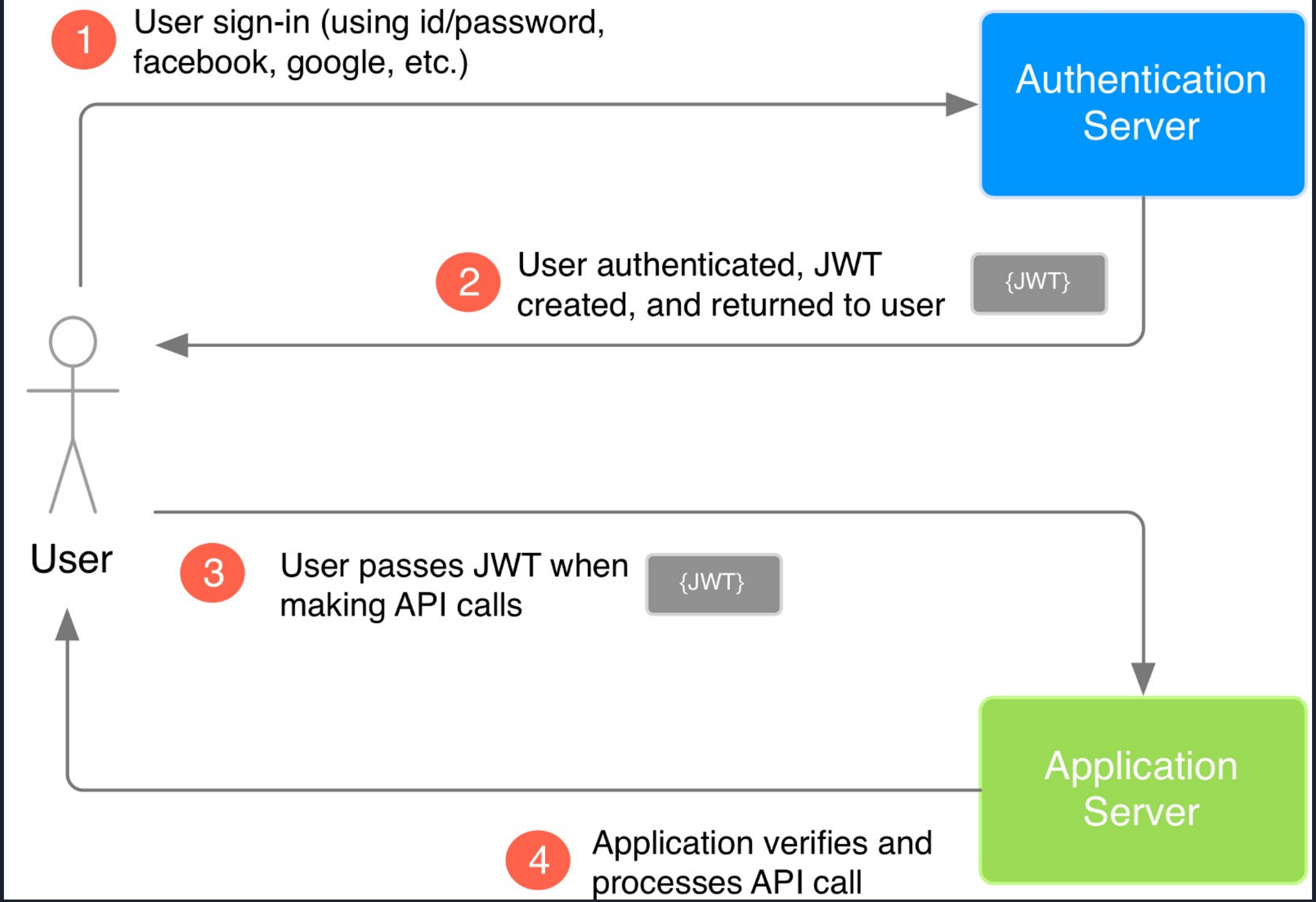
❑ Encrypted In Storage

❑ Message Integrity





Step	Client	Direction	Message	Direction	Server
1	🖥		Client Hello Supported Cipher Suites Guesses Key Agreement Protocol Key Share	>	🗄
2	🖥	<	Server Hello Key Agreement Protocol Key Share Server Finished		🗄
3	🖥		Checks Certificate Generates Keys Client Finished	>	🗄



1 User sign-in (using id/password, facebook, google, etc.)

2 User authenticated, JWT created, and returned to user

3 User passes JWT when making API calls

4 Application verifies and processes API call

5/5 - HTTP Status Codes

❑ Clear Status Codes

Building Your Own API

https://readwrite.com/2015/11/16/how-to-build-an-api-amazon-lambda/

DON'TS

Ignore Security

THANK YOU

Questions?